7-20-2020 1:00 PM

Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap

Christina Catenacci, *The University of Western Ontario*

Supervisor: Botterell, Andrew, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Law

Abstract

This dissertation argues that there is an electronic surveillance gap in the employment context in Canada, a gap that is best understood as an absence of appropriate legal provisions to regulate employers' electronic surveillance of employees both inside and outside the workplace. This dissertation aims to identify and articulate principles and values that can be used to close the electronic surveillance gap in Canada and suggests that, through the synthesis of social theories of surveillance and privacy, together with analyses of privacy provisions and workplace privacy cases, a new and better workplace privacy regime can be designed. This dissertation uses both a comparative legal doctrinal methodology concerning the legal analyses of privacy provisions and workplace privacy cases, and an interdisciplinary legal methodology regarding social theories of surveillance and privacy, to examine the jurisdictions of Canada, the United States, and the European Union. The ideas generated in the analyses are used to formulate proposed provisions for a new workplace privacy regime. This dissertation indicates how these provisions can be integrated into Canada's legal system, and provides examples of legislative provisions that could form part of a new workplace privacy regime. These proposed provisions modify and add to existing data protection legislation in Canada, such as the *Personal Information and Electronic Documents Act (PIPEDA)*. The result is a better balance of the privacy rights of employees with the legitimate business interests of employers through an effective closing of the electronic surveillance gap in employment. This dissertation contributes to a better appreciation of the role of electronic surveillance in employment, to a better understanding of the nature of electronic surveillance gap, and makes concrete suggestions about how the electronic surveillance gap can be closed by means of novel legislative provisions.

Keywords

Surveillance technologies; electronic surveillance; workplace monitoring; workplace privacy; employment; data protection; social theory; surveillance theory; privacy theory

Summary for Lay Audience

This dissertation argues that there is a need for new laws regulating the electronic surveillance of employees by employers. These new laws can be drawn from a combination of surveillance and privacy theories, and from legal analyses of privacy legislation and workplace privacy cases. This dissertation creates a new workplace privacy regime that more effectively balances the interests of the affected parties. This dissertation offers a deeper understanding of the role of electronic surveillance in the employment context and shows how new laws can more justly regulate the electronic surveillance of employees by employers.

Acknowledgments

I would like to thank my supervisor, Dr. Andrew Botterell. I was truly fortunate to meet you, and I appreciate everything that you have done for me. In just a short period of time, I learned a great deal from you. My gratitude has infinite dimensions. Thank you for believing in me.

I would like to thank Dr. Erika Chamberlain and Mary Morris. Thank you so much for your support. I could not have done this without you. I will be forever grateful for everything that you have done for me.

I would like to thank Dr. Teresa Scassa, Dr. Samuel Trosow, Dr. Anabel Quan-Haase, and Dr. Gillian Demeyere. Thank you very much for your constructive feedback. Your input was invaluable and it helped me make significant improvements to the dissertation. I will never forget what you have done for me.

I would like to thank the faculty and staff of Western Law. Thank you again for your help when I was a *FIMULAW: Interdisciplinary Connections* organizing committee member over the years; I especially enjoyed working with you last year when the event took place at Western Law. Thank you to Karen Kueneman for your support. I am so grateful that I was able to be involved with the research event, as it exposed me to countless interesting aspects of interdisciplinary work that ultimately helped me with this dissertation.

Table of Contents

List of Tables

List of Appendices

Chapter 1

1 Introduction

This Introduction describes the problem statement, the focus and justification for the dissertation, and the dissertation's objective. It then sets out the research question, hypotheses, methodology, and theoretical framework used in this dissertation.

1.1 Problem Statement

The motivation for this dissertation is my belief that Canada is falling behind when it comes to informational privacy protection. This is plain to see when reviewing the recently announced[1] joint resolution created by Information and Privacy Ombudspersons and Commissioners from across Canada, who are urging their governments to modernize privacy and access to information laws.[2] More specifically, the report states:

> Privacy and access to information are quasi-constitutional rights that are fundamental to individual self-determination, democracy and good government. New technologies have numerous potential benefits for society but they have impacted fundamental democratic principles and human rights, including privacy, access to information, freedom of expression and electoral processes.
>
> Increasingly, the public is concerned about the use and exploitation of personal information by both governments and private businesses and, in particular, the opaqueness of information handling practices. Security breaches are happening more often and have impacted millions of citizens.
>
> While it is important to acknowledge that there have been legislative advances made in some Canadian jurisdictions, there is still ongoing work required to enhance and establish consistent modernization. Most Canadian access and privacy laws have not been fundamentally changed since their passage, some more than 35 years ago. They have sadly fallen behind the

---

[1] Office of the Privacy Commissioner of Canada, "Canada's Access to Information and Privacy Guardians Urge Governments to Modernize Legislation to Better Protect Canadians" (6 November 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/>.

[2] Office of the Privacy Commissioner of Canada, "Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners" (1−2 October 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191106/>.

> laws of many other countries in the level of privacy protection provided to citizens.[3]

The report calls for improvements in the areas of privacy, access to information, and enforcement, as well as renewed commitments to collaboration and engagement to make innovative privacy and access to information changes.[4]

Indeed, United Kingdom Information Commissioner and former Information and Privacy Commissioner for British Columbia Elizabeth Denham[5] has recently commented in a podcast by Michael Geist:

> Unfortunately, Canadian law has not kept pace with the kind of reforms that we are seeing around the world…The law needs to keep up with the technology. And it's really important that regulators can take action to protect people, especially online.[6]

Denham points out that Canada does not provide comprehensive personal data protection across Canada and that further complications are created because Canada is a federated system.[7] Denham also highlights the importance of trust when dealing with privacy policy and regulation:

> People have to know that somebody has their back and there is strong protection, because you need trust. People won't go along unless they feel there is trust in the system.[8]

Many jurisdictions have made important advances in privacy protection by creating stronger data protection laws and also constitutional or human rights laws. For instance, effective May 25, 2018, the European Union enacted the *General Data Protection*

---

[3] *Ibid.*
[4] *Ibid.*
[5] Elizabeth Denham is currently (as of April, 2020) the UK Information Commissioner at the Information Commissioner's Office in Cheshire. She is the former Information and Privacy Commissioner for British Columbia, and also the former Assistant Privacy Commissioner of Canada. See Information Commissioner's Office, "Elizabeth Denham CBE, Information Commissioner" (2020), online: *Information Commissioner's Office* <https://ico.org.uk/about-the-ico/who-we-are/information-commissioner/>.
[6] Michael Geist, "The LawBytes Podcast, Episode 2: "It's Time to Modernize the Laws"" (11 March 2019) at 9m:00s–9m:45s, online (podcast): *Michael Geist* <http://www.michaelgeist.ca/2019/03/the-lawbytes-podcast-episode-2-its-time-to-modernize-the-laws/>.
[7] *Ibid* at 22m:55s–23m:20s.
[8] *Ibid* at 23m:28s–23m:41s.

Regulation (*GDPR*)[9] to accompany its broad right to privacy in Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (*EU Convention*).[10] And effective January 1, 2020, the most privacy-protective State in the United States, California, created the *California Consumer Privacy Act of 2018* (*California Consumer Privacy Act*)[11] to accompany its constitutional provision declaring a broad right to privacy in section 1 of Article 1 of the *California Constitution.*[12] California even has section 980 in its *California Labor Code,*[13] which prevents employers from forcing employees to provide usernames and passwords to their social media accounts.

Canada's private sector data protection legislation, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[14] on the other hand, has been criticized for being outdated, for not keeping up with recent technological advances, for not providing adequate order-making powers to the Privacy Commissioner of Canada, and for not being as sophisticated as the *GDPR*.[15] As a result, Canada may be unable to continue its

---

[9] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L119/1 [*GDPR*].

[10] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5 (1950), art 8 [*EU Convention*].

[11] *California Consumer Privacy Act of 2018*, 3 CIV 1.81.5 (2018) [*California Consumer Privacy Act*].

[12] Cal Const art I, § 1 [*California Constitution*].

[13] Cal Lab Code § 980 (2012) [*California Labor Code*].

[14] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

[15] Office of the Privacy Commissioner of Canada, "Privacy Commissioner Denounces Slow Progress on Fixing Outdated Privacy Laws" (27 September 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180927/>; International Association of Privacy Professionals, "Michael Geist Calls for More Robust Privacy Law at the IAPP Canadian Privacy Symposium, 2018" (13 July 2018), online (video): *YouTube* <https://www.youtube.com/watch?v=l-iIuoNqFO8>; Michael Geist, "PIPEDA at 20: Time for PIPEDA 2.0" (13 July 2018), online (blog): *Michael Geist* <http://www.michaelgeist.ca/2018/07/pipeda-at-20-time-for-pipeda-2-0/>; Office of the Privacy Commissioner of Canada, "Appearance Before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)" (16 February 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20170216/>; Timothy Banks, "Should PIPEDA be amended to meet GDPR requirements?" (4 April 2017), online: *iapp.org* <https://iapp.org/news/a/should-pipeda-be-amended-to-meet-gdpr-requirements/>; EC, *Decision 2002/2/EC Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, [2002] OJ, L002/0013; Bob Zimmer, "Towards Privacy

harmonious trade relationship with the European Union.[16] In addition, it remains unclear whether there is a constitutional or human right to privacy in Canada.[17] Privacy has historically been interpreted to be a quasi-constitutional right in public sector privacy cases concerning data protection laws,[18] and while it has recently been acknowledged by the Supreme Court of Canada as an important quasi-constitutional right that fosters and promotes a free and democratic society,[19] Canada has not yet created a right to privacy that applies throughout the country. Only one Canadian province, Québec, has clearly established a broad right to privacy in its *Charter of Human Rights and Freedoms* (*Québec Charter*).[20]

Not only is Canada behind the times when it comes to general data protections, it is also underinclusive when it comes to data protections in areas such as employment law.[21] This can be seen by noting that *PIPEDA* applies in the employment context only in connection

---

by Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics (February 2018) at 62–70, online (pdf): *House of Commons* <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf >; Office of the Privacy Commissioner of Canada, "Remarks by Privacy Commissioner of Canada Regarding the Facebook/Cambridge-Analytica investigation" (25 April 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20190425/> [Privacy Commissioner, "Remarks"].

[16] *Ibid.*

[17] *Canadian Charter of Rights and Freedoms*, s 7, Part 1 of the *Constitution Act,* 1982, being Schedule B to the *Canada Act 1982*(UK),1982, c 11; *Canadian Human Rights Act*, RSC, 1985, c H-6.

[18] The public sector privacy legislation, *Privacy Act*, RSC, 1985, c P-21, has been considered to be quasi-constitutional as seen in *Lavigne v Canada (Commissioner of Official Languages,* 2002 SCC 53 at para 24; *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 65-66, 132 FTR 55 (SCC); *HJ Heinz Co of Canada Ltd v Canada (Attorney General)*, 2006 SCC 13 at para 28. See also Michael E Power, *The Law of Privacy* (Markham: LexisNexis Canada Inc, 2013) at 13; Marta Otto, *The Right to Privacy in Employment: A Comparative Analysis* (Oxford: Hart Publishing, 2016) at 133−134.

[19] *UFCW, Local 401 v Alberta (Information and Privacy Commissioner)*, 2013 SCC 62 at para 19; *Douez v Facebook Inc*, 2017 SCC 33 at paras 58–59.

[20] *Charter of Human Rights and Freedoms*, CQLR c C-12, s 5 [*Québec Charter*].

[21] *PIPEDA*, *supra* note 14 at s 4(1). Pursuant to section 4(1), *PIPEDA* applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities; or (b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

with the operation of federal works, undertakings or businesses.[22] While there are some employment-related provisions in the substantially similar private sector data protection legislation of Alberta,[23] British Columbia,[24] and Québec,[25] this partial coverage inevitably leads to the creation of patchwork protections.[26]

In fact, Canadian employees enjoy different data protections depending on the province in which they are located, their unionization status, and what sector—public or private—they are part of.[27] The result of this piecemeal set of protections is a confusing, inconsistent, and unfair privacy regime in the Canadian employment context.

Canada's private sector data protections are also silent on the increasingly important issue of electronic surveillance. This failure amounts to a significant blind spot and creates a troubling problem, which I will call the "electronic surveillance gap". In the employment context, which is the focus of this dissertation, the electronic surveillance gap can be understood as an absence of legal provisions to regulate employers' electronic surveillance of employees inside and outside the workplace. One consequence of the electronic surveillance gap in this context is that serious issues relating to electronic surveillance of employees, such as balancing the legitimate business interests of employers with the justifiable privacy interests of employees, remaining unaddressed. This lack of direction is highlighted when one asks how this balancing of interests will take place, particularly when employers are attempting to respect the privacy of their employees while simultaneously protecting the personal information of their own clients. Accordingly, we see serious data breaches such as the recent Desjardins data breach,

---

[22] *PIPEDA*, *supra* note 14 at ss 2(1), 4(1). Some examples of federal works, undertakings or businesses to which *PIPEDA* applies include railways, banks, airlines, and radio broadcasting stations.
[23] *Personal Information Protection Act*, SA 2003, c P-6.5 [*AB PIPA*].
[24] *Personal Information Protection Act*, SBC 2003, c 63 [*BC PIPA*].
[25] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 [*QC Act*].
[26] One patch-repairing strategy is to add statutory or common law invasion of privacy torts. For instance, one example of a statutory tort of violation of privacy can be found in Saskatchewan's statute, *The Privacy Act*, RSS 1978, c P-24. One example of a common law tort of intrusion upon seclusion can be found in Ontario's landmark case, *Jones v Tsige*, 2012 ONCA 32.
[27] Otto, *supra* note 18 at 171.

which constituted the most massive data breach in Canadian history.[28] A rogue employee committed the breach; he allegedly created a scheme to win the trust of his colleagues and used their access along with his own to assemble a data trove.[29] Security experts note that this type of a data breach is not uncommon; about 33 percent of reported breaches are caused by an insider who is typically an authorized individual with valid credentials within the organization.[30]

Moreover, it appears that essential principles and values stemming from workplace privacy disputes involving the electronic surveillance of employees are nowhere to be found in *PIPEDA*.

The electronic surveillance gap is most striking when it involves parties who experience power imbalances. This is especially true when looking at the employment relationship where there is unequal bargaining power between employers and employees.[31] Simply put, employers have the potential to abuse their monitoring power and take advantage of weaker, more vulnerable employees, under the guise of exercising management rights in the workplace.[32] Indeed, the employment relationship has been considered by Elizabeth Denham, who was then acting as Information and Privacy Commissioner for British

---

[28] Jonathan Montpetit, "Personal Data of 2.7 Million People Leaked from Desjardins" (20 June 2019), online: *CBC News Montreal* <https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297>.
[29] *Ibid*.
[30] Buckley Smith, "Laying Blame on Employee in Desjardins Data Breach is Ignoring the Big Picture, Security Experts Say" (21 June 2019), online: *ITWorldCanada* <https://www.itworldcanada.com/article/laying-blame-on-employee-in-desjardins-data-breach-is-ignoring-the-big-picture-security-experts-says/419299>.
[31] *Machtinger v HOJ Industries Ltd*, [1992] 1 SCR 986 at para 31, 1992 CarswellOnt 892 (SCC) [*Machtinger*]; *Wallace v United Grain Growers Ltd*, [1997] 3 SCR 701 at paras 92−93, 1997 CarswellMan 455 (SCC) [*Wallace*]. See also David J Doorey, *The LAW of Work: Common Law and the Regulation of Work* (Toronto: Emond Montgomery Publications Limited, 2016) at 5−6, 67−75, 111−120 [David Doorey, "Common Law and Regulation"]; David J Doorey, *The LAW of Work: Industrial Relations and Collective Bargaining* (Toronto: Emond Montgomery Publications Limited, 2017) at 67, 94−97, 239−241 [David Doorey, "Industrial Relations and Collective Bargaining"].
[32] Peter Kivisto, *Social Theory: Roots & Branches*, 5th ed (Oxford: Oxford University Press, 2013) at 3–38; Carsten Bagge Laustsen et al, *Social Theory: A Textbook* (London: Routledge, 2017) at 14−34, online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315657998>; Nick Dyer-Witheford, *Cyber-Proletariat: Global Labour in the Digital Vortex* (Toronto: Between the Lines, 2015) at 4−15, 19−38.

Columbia, to be the ideal privacy laboratory.[33] This is because there is a blurring of workplace and personal digital devices as well as a blurring of work and personal time;[34] because the parties must work together to coexist for significant periods of time despite the presence of significant opposing interests;[35] because the parties are privy to several details regarding each other's personal lives;[36] and because employer surveillance activities can negatively affect the employment relationship by aggravating the lack of trust between the parties and create chilling effects on employee morale.[37]

What the foregoing discussion highlights is an increased need to build trust between employers and employees, something that can be done by creating stronger data protections for employees.[38] Unfortunately, Canadian privacy protections remain weak in this regard. Although the employment relationship requires protective data protection provisions that can minimize the abuse of power and effectively restore trust in the relationship,[39] such provisions have not yet been created.

Despite the clear power imbalances that employers and employees experience, there is no acknowledgement in *PIPEDA* that employees are often not in a position to validly provide, withhold, or revoke their consent in response to employers' decisions to conduct

---

[33] Elizabeth Denham, "The Employment Relationship as the Privacy Laboratory" (22 November 2013), online: *Office of the Information and Privacy Commissioner for British Columbia* <https://www.oipc.bc.ca/speeches/1584> at 2.
[34] *Ibid* at 5–9; Government of Canada, "Disconnecting From Work-Related E-Communications Outside of Work Hours: Issue Paper" (4 April 2019), online: *Government of Canada* <https://www.canada.ca/en/employment-social-development/services/labour-standards/reports/disconnecting-e-communications.html>; Office of the Privacy Commissioner of Canada, "Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?" (22 July 2015), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/>; Lysa Appleton, "Flex Work and Telecommuting" (2018), online: *Career Professionals of Canada* <https://careerprocanada.ca/flex-work-telecommuting/>; Nathan Battams, "Out of the office: workshifting and remote work in Canada" (August 2013) at 1, online (pdf): *The Vanier Institute: Fascinating Families* <http://vanierinstitute.ca/wp-content/uploads/2015/11/FFAM_2013-08-00_Workshifting-and-remote-work-Canada.pdf>.
[35] Denham, *supra* note 33 at 2.
[36] *Ibid* at 2–3.
[37] *Ibid* at 3, 9−10; Jennifer Stoddart, "Annual Reports to Parliament 2004 on the Personal Information Protection and Electronic Documents Act" (October 2005), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/200405/2004_pipeda/>.
[38] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018) at 74.
[39] *Ibid* at 50–52, 61, 67–69, 71.

electronic surveillance of employees. Likewise, there is no acknowledgment that employers may only engage in reasonable acts of surveillance based on the legitimate business interests of employers and the privacy interests of employees. Employees have no real voice with respect to the extent to which employers conduct electronic surveillance. These features are simply not included in the legislation.[40]

In fact, *PIPEDA* allows employers to unilaterally collect, use and disclose personal information without the consent of employees if the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the employers and employees, and employers inform employees that the personal information will be or may be collected, used or disclosed for those purposes.[41] There is no definition accompanying the phrase, "necessary to establish, manage or terminate an employment relationship".[42] And being informed of a privacy violation that will or may soon take place cannot possibly constitute fair and proper notification to employees.

To date, the federal government's responses to these sorts of concerns have been problematic. For example, the government's recent attempt to introduce a so-called Digital Charter[43] does not adequately protect the privacy interests of Canadians. To be sure, there is an acknowledgment of the need to simultaneously allow for innovation and protect users from data misuse, but simply listing 10 principles[44] does not adequately or effectively address the electronic surveillance gap in employment.[45] By not acting,

---

[40] *PIPEDA*, *supra* note 14 at ss 6.1, 7(1), 7(2), 7(3), Schedule 1, cl 4.3.
[41] *Ibid* at s 7.3.
[42] *Ibid* at ss 2(1), 7.1(1).
[43] Government of Canada, "Canada's Digital Charter: Trust in a Digital World" (21 May 2019), online: *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>; Government of Canada, "Canada's Digital Charter: Trust in a Digital World" (21 May 2019), online (video): *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.
[44] The ten principles include: Universal Access; Safety and Security; Control and Consent; Transparency, Portability and Interoperability; Open and Modern Digital Government; A Level Playing Field; Data and Digital for Good; Strong Democracy; Free from Hate and Violent Extremism; and Strong Enforcement and Real Accountability. See Government of Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians" (21 May 2019), online: *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html>.
[45] I assert that the same is true for the recent Mandate Letter to the Minister of Innovation, Science and Industry. See Office of the Prime Minister, "Minister of Innovation, Science and Industry Mandate Letter" (December, 2019), online: *Prime Minster of Canada* <https://pm.gc.ca/en/mandate-letters/minister-innovation-science-and-industry-mandate-letter>.

Canada risks missing an opportunity to be a world leader when it comes to addressing the electronic surveillance gap and enabling employees to preserve a sense of dignity and self-respect.

1.2 Focus

The focus of this dissertation is limited to workplace privacy involving electronic surveillance technologies that affect the employment relationship.

This dissertation will focus in particular on two main instances of electronic surveillance that arise in the workplace. For simplicity, I will call these "surveillance scenarios".[46]

The first surveillance scenario involves what I will call "proactive surveillance operations". In such situations, employers become suspicious of employees, believing that they are being dishonest about something (such as an injury or illness), and decide to instigate surveillance to confirm their suspicions. Such cases can involve taking steps to access information about employees by hiring outside private investigators who use specialized equipment such as cameras, audio equipment, or particular software that can analyze online use with web browsing surveillance technology (for instance, using snapshot or keystroke activity monitoring). Employers may take measures to install overt or covert cameras in the workplace, contact a data profiler to view aggregated data from social media activity, or purchase other equipment to track their company vehicles or property to catch an employee's actions, including Global Position System (GPS), Radio Frequency Identification (RFID), web cameras, video cameras, closed-circuit television (CCTV), or telematics equipment.

The second surveillance scenario involves what I will call the "discovery of employee misuse of technology". This misuse of technology can harm the employer (such as some action taken online that can harm the employer's reputation) and can take place on-duty or off-duty using work or personal digital devices. These scenarios can involve employers accessing information regarding an employee's misuse of company

[46] See Chapter 2 regarding the examination of surveillance theories.

technology in several ways, including reviewing details provided by corporate computer cache logs, hard drives or Universal Serial Bus (USB) storage keys, emails that are copied to the server, phone records, and GPS activity logs. It can also involve employers accessing information regarding an employee's misuse of technology by examining the employee's digital devices that can be fluidly on the move inside or outside the workplace, or online activity that is generated during or outside working hours.

1.2.1 Justification

There are three principal reasons why this dissertation is limited to the employment context. The first reason is because the employment relationship is the most suitable setting for studying and understanding electronic surveillance technologies as they affect relationships of power imbalances. As discussed above, there is a significant potential for employers to abuse their electronic surveillance power and take advantage of vulnerable employees.

The second reason why this dissertation is limited to the employment context is because there is a rich body of case law stemming from workplace privacy cases that can provide significant insights about how to best create an effective privacy regime pertaining to electronic surveillance technologies.

The third reason why this dissertation is limited to the employment context is because of the centrality of paid work to the lives of individuals. One thing that the law is uniquely placed to do is protect essential values, including the dignity and self-respect of employees, in the employment sphere. This was eloquently put by Dickson C.J. in the *Alberta Reference*:[47]

> Work is one of the most fundamental aspects in a person's life, providing the individual with a means of financial support and, as importantly, a contributory role in society. A person's employment is an essential component of his or her sense of identity, self-worth and emotional well-being. Accordingly, the conditions in which a person works are highly

[47] *Reference Re Public Service Employee Relations Act (Alta),* [1987] 1 SCR 313, 1987 CarswellAlta705 (SCC) [*Alberta Reference*].

> significant in shaping the whole compendium of psychological, emotional and physical elements of a person's dignity and self-respect.[48]

To be sure, employment operates against the backdrop of a larger sphere of interactions between individuals, corporate entities, and governments that is also affected by privacy laws.[49] There is a general problem with the electronic surveillance gap, and employment is the ideal realm for studying the problem. The electronic surveillance gap arises in interesting and important ways in the unique employment sphere. Accordingly, the narrow focus of this dissertation is employment because it allows for a useful way of understanding the electronic surveillance gap. The present examination is properly situated within the examination of the privacy protections in the employment relationship.

Current approaches to privacy do not appear to provide protections that are adequate to close the electronic surveillance gap. For example, the dominant approach—which simply relies on existing data protection provisions—is insufficient to adequately address the sorts of specific and unique issues that arise from using electronic surveillance technologies. This results in a lack of clarity regarding the extent of privacy protection with respect to increasingly intrusive electronic surveillance technologies, and raises questions as to how to sufficiently close the electronic surveillance gap in employment.

This dissertation suggests that, through the synthesis of social theories involving surveillance and privacy, together with analyses of legislative privacy and electronic surveillance protections ("privacy provisions"), court decisions, and labour arbitrations

---

[48] *Ibid* at para 95.

[49] One example of an electronic surveillance issue in the larger sphere that has affected Canadians is the notorious Facebook-Cambridge Analytica data scandal of 2018 that involved the collection of personally identifiable information of approximately 50 million user profiles of Facebook users without consent to use for political and advertising purposes. See Roger McNamee, *Zucked* (New York: Penguin Press, 2019) at 178–240; Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (24 July 2019), online: *Federal Trade Commission* <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>; Catherine Tunney, "Privacy Watchdog Taking Facebook to Court, Says Company Breached Privacy Laws" (25 April 2019), online: *CBC News* <https://www.cbc.ca/news/politics/privacy-watchdog-cambridge-analytica-facebook-1.5110304>; Privacy Commissioner, "Remarks", *supra* note 15; Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights" (21 November 2019) at 27−38, online (pdf): *Amnesty International* <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>.

("workplace privacy cases"), a new and improved regime that closes the electronic surveillance gap ("workplace privacy regime") can be designed. This dissertation makes a significant contribution to how we view electronic surveillance in employment, how we understand the electronic surveillance gap, and how we can close the electronic surveillance gap by means of novel legislative provisions. The proposed legislative provisions better protect the dignity and self-respect of employees, while still allowing employers to responsibly use their electronic surveillance power to achieve their business goals. The proposed legislative provisions have the potential to enhance trust in the employment relationship, minimize chilling effects on employee morale, and ensure that employment can provide a sense of meaning, dignity, and self-respect to employees, free from concerns about inappropriate intrusions into their private lives.

1.3 Objective

The objective of this dissertation is to determine how the principles and values that emerge from selected privacy provisions and workplace privacy cases can be used to close the electronic surveillance gap using a design that fits into Canada's legal system.

1.4 Research question

How can the principles and values that emerge from selected privacy provisions and workplace privacy cases be used to close the electronic surveillance gap using novel legislative provisions?

1.5 Hypotheses

This dissertation will suggest that there are currently insufficient data protection provisions in Canada's legal regime for closing the electronic surveillance gap.

This dissertation will also argue that principles and values can be extracted from selected privacy provisions and workplace privacy cases, and can be used to design a new workplace privacy regime containing proposed legislative provisions that closes the electronic surveillance gap in a way that fits into Canada's current legal system. These proposed provisions modify and add to Canada's data protection provisions.

1.6 Methodology

This dissertation uses two main methodologies. The primary methodology is a comparative legal doctrinal methodology. Additionally, an interdisciplinary methodology is used in this dissertation to examine social theory. Therefore, this methodology section will include a discussion of: (1) Legal Analysis: Comparative Legal Doctrinal (regarding Chapters 4 and 5); and (2) Social Theory: Interdisciplinary (concerning Chapters 2 and 3).

1.6.1 Legal Analysis: Comparative Legal Doctrinal

The primary methodology in this dissertation is a legal doctrinal methodology, and it is used for Chapters 4 and 5, where legal analyses of privacy provisions and workplace privacy cases will be undertaken. This methodology is based on the idea that legal research is an iterative process of problem-solving that requires legal reasoning and analysis.[50] In fact, the manner in which one uses legal authorities to build legal arguments requires mastery of all the fundamental components of legal reasoning including critical interpretation and strategic application—when done correctly, legal research can lead to creative, imaginative, and flexible problem solving.[51]

The doctrinal methodology that is used in this dissertation emphasizes both primary legal material (cases and legislation) and secondary material.[52] The doctrinal method is a two-part process involving locating sources of law and subsequently interpreting and analyzing them.[53] In terms of purpose and motivation for undertaking the work, this dissertation uses a normative purpose; in particular, the research goes beyond simply describing what the law is, and argues for legal change.[54]

---

[50] Sarah Valentine, "Legal Research as a Fundamental Skill: A Lifeboat for Students and Law Schools" (2010) 39 Baltimore L Rev 173 at 210.
[51] *Ibid* at 211, 219.
[52] Chris Dent, "A Law Student-Oriented Taxonomy for Research in Law" (2017) 48 VUWLR 371 at 377.
[53] Terry Hutchinson, "Doctrinal Research" in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 8 at 18.
[54] Dent, *supra* note 52 at 386–387; Shane Kilcommins, "Doctrinal Legal Method (Black-Letterism): Assumptions, Commitments and Shortcomings" in Laura Cahillane & Jennifer Schweppe, eds, *Legal Research Methods: Principles and Practicalities* (Dublin: Clarus Press Ltd, 2016) 7 at 9−11.

With respect to the scope of this dissertation, selected workplace privacy laws in private sector workplaces in Canada, the United States, and European Union jurisdictions are examined. The private sector is examined because it is beneficial to maintain a reasonably sized project, delve deeper into the one sector, and analyze what is—at least in my opinion—the more interesting sector compared to the public sector.[55] I say this because analysis of the private sector elicits more intriguing questions regarding the responsibilities of private companies. As a result, certain specialized sectors and contexts such as government, health, and criminal law are not examined in this dissertation. Both unionized and nonunionized workplaces are examined when considering the two surveillance scenarios involving court decisions and labour arbitrations (torts, findings of the Privacy Commissioners, and decisions of the National Labour Relations Board are not examined in this dissertation).

To that end, in this dissertation a comparative approach to the legal doctrinal method is used, which involves comparing "the law of different jurisdictions, legal families or legal traditions, with a special eye on the similarities and differences".[56] The rationale for using a comparative doctrinal approach is to discover any possible benefits and also warnings of possible difficulties when comparing jurisdictions, and in so doing, deepening the understanding of the Canadian system while trying to improve it.[57] One strategy is to compare similarities and differences between laws of the different jurisdictions, and determine whether the laws achieve the same function, while also being sensitive to the cultural context of the jurisdictions examined.[58] Not only does function assist in

---

[55] For the purposes of this discussion, the public sector involves government of Canada departments and agencies, provincial ministries and agencies, and municipal departments. For example, see Government of Canada, "Departments and agencies" (31 July 2017) online: *Government of Canada* <https://www.canada.ca/en/government/dept.html> and Government of Ontario, "Provincial ministries and agencies" (2017) online: *Government of Ontario* <https://www.ontario.ca/data/provincial-ministries-and-agencies>.

[56] Jaap Hage, "Comparative Law as Method and the Method of Comparative Law" in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 37 at 37−38.

[57] Dent, *supra* note 52 at 384–385.

[58] Geoffrey Samuel, "Comparative Law and its Methodology" in Watkins & Burton, *supra* note 53, 121 at 124–134; Mark Van Hoecke, "Methodology of Comparative Legal Research", Law & Method (December 2015) 1 at 3−6, 11, 28, 30, online: *Law and Method* <http://www.lawandmethod> DOI:

identifying cross-jurisdictional legal materials for mutual comparison, but it also provides interesting angles from which to analyze the materials.[59]

To be sure, there have been criticisms of the doctrinal legal methodology.[60] According to these criticisms, the doctrinal research method is less compelling than the research methods used by those in the sciences and social sciences.[61] The criticisms suggest that law is a social endeavor, and the strict application of rules can mask phenomenon operating in society.[62] Consequently, there has been a growth in the use of non-doctrinal and interdisciplinary research work by legal academics.[63] As can be seen in the discussion below regarding interdisciplinary methods, I agree that interdisciplinary research approaches can bolster doctrinal legal methodology and lead to innovative research outcomes.

For this dissertation, I propose to focus on privacy provisions and a variety of workplace privacy cases that are a source for principles and values relevant to designing a proposed new workplace privacy regime. My claim is that these principles and values can be codified and transformed into proposed legislative provisions that can fit into the Canadian legal system.

The selected provisions provide excellent examples of privacy provisions and workplace privacy cases that highlight issues regarding the electronic surveillance gap. The privacy provisions involve different areas of law that are relevant to privacy (what I will call the "features of privacy provisions"): (1) constitutional and human rights provisions; (2) data protection provisions; and (3) employment provisions. Correspondingly, workplace privacy cases have several aspects that provide insights into a workplace privacy situation

---

<10.5553/REM/.000010>; Mathias M Siems, "The Curious Case of Overfitting Legal Transplants" in Adams & Heirbaut, *supra* note 56, 133 at 136−138.

[59] Catherine Valcke & Mathew Grellette, "Three Functions of Function in Comparative Legal Studies" in Adams & Heirbaut, *supra* note 56, 99 at 106−109, 111.

[60] Hutchinson, *supra* note 53 at 9, 21–25.

[61] *Ibid*.

[62] Kilcommins, *supra* note 54 at 15, 17.

[63] Hutchinson, *supra* note 53 at 10.

(what I will call the "features of workplace privacy cases"): (1) employee success in the wrongful termination/privacy claim versus failure in the claim; (2) court versus labour arbitrator; (3) surveillance scenario (proactive surveillance operations versus discovery of employee misuse of technology); (4) electronic surveillance technology type; and (5) on-duty versus off-duty conduct.

This dissertation is limited to the examination of selected privacy provisions and workplace privacy cases, with an aim of presenting a balanced representation and a strategic combination of the features of privacy provisions and features of workplace privacy cases. This will ensure that the analysis will generate relevant insights into how to close the electronic surveillance gap for the creation of a proposed workplace privacy regime.

Put another way, the goal is not to provide an exhaustive description of the entire legal landscape in Canada, the United States, and European Union when it comes to privacy. Rather, the goal is to engage in a nuanced discussion of the chosen privacy provisions and workplace privacy cases to glean information relevant to the construction of a new workplace privacy regime.

First, the privacy provisions from Canada will be selected from the: *Québec Charter*;[64] *PIPEDA*[65] (including the *PIPEDA Breach Regulations*[66]); *BC PIPA*;[67] and *QC Act*.[68] There will also be a discussion of Canada's *Bill S-21 (Privacy Rights Charter)*.[69] The privacy provisions from the United States will be chosen from the: *California Constitution*;[70] *California Consumer Privacy Act*;[71] *California Labor Code*,[72] and

---

[64] *Supra* note 20.
[65] *Supra* note 14.
[66] *Breach of Security Safeguards Regulations* (SOR/2018-64) [*PIPEDA Breach Regulations*].
[67] *Supra* note 24.
[68] *Supra* note 25.
[69] Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess, 37th Parl, 2001 (first reading 13 March 2001, dropped from the Senate Order Paper in 2002) [*Bill S-21 (Privacy Rights Charter)*].
[70] *Supra* note 12.
[71] *Supra* note 11.
[72] *Supra* note 13.

California Civil Code (Customer Records).[73] There will also be an examination of provisions in these American bills: *Bill S5642 (New York Privacy Act);*[74]and *Bill SB 6280 (Washington Facial Recognition).*[75] The privacy provisions from the European Union will come from the: *EU Convention*;[76] and the *GDPR*.[77] Chapter 4 elaborates on the reasons why these privacy provisions have been selected for the analysis.

In order to maintain the focus and narrow scope of the dissertation, it will be necessary to compare a small number of provisions regarding similar common topics. A mix of selected privacy provisions of the various jurisdictions will be discussed under each of three themes: (1) foundational principles touching on privacy and electronic surveillance;[78] (2) consent and balancing rights with legitimate interests;[79] and (3) order-making powers, penalties, and fines.[80]

Second, the two workplace privacy cases chosen from Canada are: *Steel* [81] and *Maxam Bulk Services*.[82] The two workplace privacy cases selected from the United States are:

---

[73] Cal Civ Code, 3 CIV 1.81 (2000) [*California Civil Code (Customer Records)*].
[74] US, SB 5642, *New York Privacy Act*, 2019−2020, Reg Sess, NY, 2019 [*Bill S5642* (*New York Privacy Act)*]. Bill S5642 was introduced into the Senate, read twice on May 9, 2019 and January 8, 2020, and referred to the Committee on Consumer Protection on those dates. See New York State Senate, "Senate Bill S5642" (2020) online: *New York State Senate* <https://www.nysenate.gov/legislation/bills/2019/s5642>.
[75] US, SB 6280, *Concerning the Use of Facial Recognition Services*, 2019−2020, Reg Sess, Wash, 2020 (passed by the Senate and the House on March 12, 2020 and signed by the Governor but with a partial veto on March 31, 2020; sections 1 to 9 and sections 11 to 13 become effective July 1, 2021 and will form part of RCW, Title 43, Chapter 257) [*SB 6280 (Washington Facial Recognition)*]. See also Washington State Legislature, "Bill Information: SB 6280" (12 April 2020), online: *Washington State Legislature* <https://app.leg.wa.gov/billsummary?BillNumber=6280&Initiative=false&Year=2019>.
[76] *Supra* note 10.
[77] *Supra* note 9.
[78] The following provisions will be discussed for theme (1): *PIPEDA*, s 3, Schedule 1, cl 4.2, 4.4; *Québec Charter*, s 5; *Bill S-21 (Privacy Rights Charter)*, ss 1−5; *California Consumer Privacy Act*, § 1798.140; *Bill S5642* (*New York Privacy Act)*, § 1102; *Bill SB 6280* (*Washington Facial Recognition)*, §§ 1, 2, 3, 8, 11; *California Constitution*, art 1, § 1; *GDPR*, arts 1, 4, 5, 9, 21, 22, 23, 25, 35; *EU Convention*, art 8. See Appendix A.
[79] The following provisions will be discussed for theme (2): *PIPEDA*, ss 2(1), 6.1, 7(1)−7(3), 7.1–7.4 10.1–10.3, Schedule 1, cl 4.3; *PIPEDA Breach Regulations*, ss 2–6; *QC Act*, s 14; *BC PIPA*, ss 7−9, 13, 16, 19; *California Consumer Privacy Act*, §§ 1798.120, 1798.125, 1798.145; *California Labor Code*, § 980; *California Civil Code (Customer Records)*, §§1798.81.5, 1798.82; *GDPR*, arts 4, 6−7, 33−34, 88. See Appendix B.
[80] The following provisions will be discussed for theme (3): *PIPEDA*, ss 14–16, 17.1–17.2, 28; *BC PIPA*, ss 52–53, 56–57; *QC Act*, ss 55, 58, 91–93; *California Consumer Privacy Act*, §1798.155; *GDPR*, arts 58, 83–84. See Appendix C.
[81] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127, aff'g 2013 BCSC 527 [*Steel*].

Graphic Packaging[83] and *Baker Hughes.*[84] And the two workplace privacy cases chosen from the European Union are: *Bărbulescu*[85] and *López Ribalda*.[86] Chapter 5 elaborates on the reasons why these workplace privacy cases have been selected for the analysis.

1.6.2 Social Theory: Interdisciplinary

Currently, it is common for many areas of legal research and scholarship to employ information and methodologies from other academic fields.[87] Legal scholarship has experienced an increased integration and cross-fertilization with other disciplines, and there has been a shift away from merely doctrinal legal scholarship towards more interdisciplinary legal scholarship, largely in response to criticisms of the doctrinal legal methodology.[88]

An interdisciplinary methodology is used in Chapters 2 and 3 to examine social theories of surveillance and privacy. This discussion is included in the dissertation because social theory plays an important role when studying law and society; it can produce a more holistic understanding of what problems the law can solve, and can contribute to the crafting of a more effective legal regime for citizens in that society.[89] Put another way, theories of surveillance and privacy can provide a foundation on which I can draw when analyzing privacy provisions and workplace privacy cases, extracting from those

---

[82] *Maxam Bulk Services and International Union of Operating Engineers, Local 115 (Lebrun) (2015)*, 2015 CarswellBC 2277, 257 LAC (4th) 402 (Arbitrator: McConchie) [*Maxam Bulk Services*].
[83] *In re Graphic Packaging International, Inc and Graphic Communications Conference International Brotherhood of Teamsters Local 77-P*, 134 LA (BNA) 369 (2014) (Wolff, Arb) [*Graphic Packaging*].
[84] *In re Baker Hughes, Inc (Claremont, OK) and United Steelworkers International Union Region VII, Local 13-391*, 128 LA (BNA) 37 (2010) (Baroni, Arb) [*Baker Hughes*].
[85] *Bărbulescu v Romania*, Application 61496/08, Judgment of the Court (Grand Chamber), 5 September 2017, rev'g Application 61496/08, Judgment of the Court (Fourth Section), 12 January 2016 [*Bărbulescu*]
[86] *López Ribalda and Others v Spain*, Applications 1874/13 and 8567/13, Judgment of the Court (Grand Chamber), 17 October 2019, rev'g Applications 1874/13 and 8567/13, Judgment of the Court (Third Section), 9 January 2018 [*López Ribalda*].
[87] David A Hollander, "Interdisciplinary Legal Scholarship: What Can We Learn from Princeton's Long-Standing Tradition?" (2007) 99 Law Libr J 771 at 771.
[88] *Ibid* at 771–775.
[89] Darren O'Donovan, "Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls" in Cahillane & Schweppe, *supra* note 54, 107 at 108, 116.

provisions and cases various principles and values, and proposing a new workplace privacy regime.

The term "socio-legal" refers to an approach to the study of law that views law as in part a social phenomenon.[90] Socio-legal studies can be invaluable because they allow for diverse methods and perspectives to be adopted by legal scholars.[91] Socio-legal studies embraces various disciplines because there is a recognition that law is not an autonomous force to which society is subjected, but rather it shapes and is shaped by broader social issues.[92] In fact, some believe that the fact that the typical law syllabus rarely includes any significant study of the theories or research methods that are regarded as fundamental by other disciplines is problematic for the future development of the legal discipline.[93] I agree that there is a range of theoretical work upon which a socio-legal researcher can draw in order to examine legal phenomena, and this is especially the case when it comes to the study of electronic surveillance and privacy.[94]

Not only is it important for law to be open to the kinds of insights that sociology can provide, but it is also important for sociology to be open to insights emerging from the study of law; the two disciplines complement each other.[95] In fact, some believe that the most valuable asset of socio-legal research is its ability to highlight issues that neither law nor sociology can articulate or study alone.[96] In this interdisciplinary space, socio-legal research is still in its infancy and creates a large potential for law and sociology to learn from each other and generate new knowledge.[97]

In my view, it is important to have a thorough understanding of social theory *and* law in order to more fully appreciate the questions raised in this dissertation. By studying social

---

[90] Fiona Cownie & Anthony Bradney, "Socio-Legal Studies" in Watkins & Burton, *supra* note 53, 40 at 42.
[91] *Ibid* at 42–43.
[92] O'Donovan, *supra* note 89 at 109.
[93] Cownie & Bradney, *supra* note 90 at 45.
[94] *Ibid* at 45–46.
[95] Reza Banakar, *Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity* (Lund, Sweden: Springer, 2015) at 37, online: *Springer* <www.springer.com>, DOI: <10.1007/978-3-319-09650-6>.
[96] *Ibid* at 38.
[97] *Ibid*.

theories of surveillance and privacy, it is possible to develop a deeper sense of the problem of the electronic surveillance gap in employment and generate unique insights when performing the legal analyses of the privacy provisions and the workplace privacy cases. I believe that reflecting on social theories of surveillance and privacy will lead to a higher likelihood of creating effective legislative provisions when crafting the proposed workplace privacy regime.

For instance, Chapter 2 is written from a capitalist surveillance perspective of surveillance, which stresses the dangers of electronic surveillance. In particular, surveillance-based capitalism involves private-sector companies engaging in the extraction of individuals' personal data to exploit their personal information. Theorists point out the dangers of ubiquitous surveillance as it relates to the general sphere outside employment, and also workplace monitoring as it relates to electronic surveillance inside the workplace. Many draw on panoptic concepts when highlighting the potential for an abuse of electronic surveillance power. The Chapter also stresses the consequences of the exploitation concerning the panoptic sort, which involves dangerous outcomes involving discrimination and profiling.

Chapter 2 begins with a discussion of the origins of surveillance with the Panopticon. This discussion highlights the potential of the exploitation of power and manipulation when conducting surveillance. Subsequently, Chapter 2 articulates the nature of electronic surveillance and the pervasiveness of everyday surveillance in the general sphere. This is important because employees operate in the general sphere during their off-duty conduct; aspects of their private lives can be detected using electronic surveillance technologies outside work and subsequently affect their status inside the workplace, and this can lead to exploitation and discrimination. The capitalist surveillance perspective highlights the high potential for exploitation to control behaviour using manipulation, domination, and power. The discussion regarding the panoptic sort emphasizes the potential for discrimination against minority groups including racialized individuals; there is also a potential for exploitation of women as described by feminist surveillance theorists.

Theories that consider surveillance in the workplace review the reasons for conducting surveillance, the technologies used to monitor employees, and the competing interests of employers and employees at work. This discussion allows one to grasp the complicated nature of electronic surveillance in the workplace and the effect of electronic surveillance on employees on a psychological level. Chapter 2 reinforces the view that there is a serious potential for employers to exploit their electronic surveillance powers and take advantage of their vulnerable employees using electronic surveillance. This Chapter also underscores the fact that current understandings of privacy do not articulate a conception of privacy that can protect individuals from unreasonable intrusions.

Chapter 3 investigates several privacy theories and asks the question, "What is privacy?" The social theories provide an understanding of what is being analyzed when studying the privacy provisions and workplace privacy cases. Further, these theories help to explain what is being protected with the newly proposed legislative provisions.

During the analysis of the social theories of privacy, the problem of conceptualizing privacy is approached from different angles to create a rich knowledge base from which to draw during the subsequent legal analyses. Reductionist theorists are critical of singling out privacy as a right, whereas non-reductionist theorists believe there is some coherent value in privacy, but disagree about how the value is conceptualized. This difference is noteworthy because the framing of the concept of privacy affects legal analyses of privacy provisions and workplace privacy cases.

While some reductionist theories understand privacy as a cluster-of-rights instead of a single right, another reductionist theory, the economic perspective on privacy, considers privacy to be useful and worth protecting only if it creates value in a data exchange.

Non-reductionist theories are more impactful since they attach a value to privacy. One theory explains the idea of privacy as a tort, discussing a right to be free of privacy intrusions. Other theories consist of discussions regarding the feminist legal theory of privacy and shed light on the darker side of privacy, where privacy may be used as a shield to conceal the negative treatment of women. Several theorists also discuss the idea of privacy as control-over-information, and this helps to understand modern societal

struggles between data owners and those who wish to manipulate and control through the use of electronic surveillance. The pragmatic contextual approach to privacy emphasizes the importance of understanding complicated privacy issues in a flexible and practical manner.

The dignity/human rights approach to privacy, the approach that I prefer, is different from all of the other theoretical approaches to privacy. This perspective of privacy provides an appropriate understanding of privacy and allows for a purposive interpretation that does not ignore the interests of the most vulnerable citizens. Chapter 3 aims to understand on a deeper level the nature of dignity, trust, and how individuals are inherently worthy and deserving of privacy. The animating idea is that individuals are not means to an end, but rather ends in themselves. Privacy is not used to get something and create value during an exchange. When looking at privacy with this lens, one can see that the interpretation of privacy provisions and workplace privacy cases will take a different route compared to others such as the economic theory of privacy. Not only does this affect the interpretation of privacy in a legal analysis, but it also influences how one may draft a new workplace privacy regime.

1.7 Theoretical Framework

This dissertation takes a capitalist surveillance theoretical approach to electronic surveillance. This approach highlights the dangers involving the abuse of electronic surveillance power. In particular, this approach to electronic surveillance argues that, since there is a high potential for employers to exploit vulnerable employees by taking advantage of their electronic surveillance power, it is necessary to provide employees with the proper protections by closing the electronic surveillance gap.

This dissertation also adopts a dignity/human rights approach to privacy. I argue, in other words, that adequate privacy protections that respect the dignity of employees are not currently in place in Canada, and they must be created and implemented as soon as possible to close the electronic surveillance gap.

1.8 Organization of the dissertation

This dissertation has an Introduction, five Chapters, and a Conclusion.

The introductory Chapter 1 describes the problem statement, the focus and justification for the dissertation, and the dissertation's objective. Following this, it sets out the research question, hypotheses, and methodology used in this dissertation. The detailed methodology section explains the comparative legal doctrinal methodology (concerning the legal analyses) and interdisciplinary legal methodology (regarding social theory) used in this dissertation. Lastly, Chapter 1 sets out the theoretical framework that is used in this dissertation.

Chapter 2 explores surveillance theories from a capitalist surveillance theoretical framework. The examination commences with understanding the beginnings of surveillance with the Panopticon, and moves through a discussion regarding the dangers of ubiquitous surveillance, the struggles regarding surveillance in the workplace, and the problems with surveillance theorists' views of privacy. Chapter 2 argues that there is a serious potential for employers to exploit their electronic surveillance powers and take advantage of their vulnerable employees using electronic surveillance. Employers have the potential to take advantage of the electronic surveillance technologies involved in ubiquitous surveillance as they pertain to off-duty conduct, and also directly in the workplace with electronic surveillance as they concern on-duty conduct. Chapter 2 concludes that conceptualizations of privacy by surveillance theorists are inadequate and it is clear that privacy rights, as envisioned by privacy theorists in Chapter 3, must be created and upheld for all individuals in society.

Chapter 3 investigates privacy theories from a dignity/human rights theoretical perspective of privacy. It advances the claim that it is necessary to proceed with a dignity/human rights approach when answering the question, "What is privacy?" Regardless of whether they are reductionist or non-reductionist, most privacy theories are problematic because they do not appropriately capture the concept of privacy. It is only the dignity/human rights approach to privacy that provides an appropriate understanding of privacy and allows for a purposive interpretation that does not leave the most

vulnerable citizens behind. Recognizing that privacy is fundamental, this flexible approach helps law drafters and decision makers make incremental modifications to adapt with an evolving society and also to achieve appropriate balances when assessing competing interests. Chapter 3 highlights the importance of using the dignity/human rights approach to treat individuals as ends and not means.

Chapter 4 examines selected privacy provisions, organized thematically, from Canada, the United States, and the European Union. Three themes, each containing selected privacy provisions of the various jurisdictions, have been created in order to compare a small number of provisions regarding common topics that are important for understanding how to close the electronic surveillance gap. First, I note the provisions that fall within each theme. Second, I analyze the provisions of each theme and discuss the principles and values that emerge from the analysis. The analysis contains a thorough examination of privacy provisions that ties into the discussion various relevant social theory ideas involving surveillance and privacy. Third, I set out ideas for incorporating the detected principles and values into the proposed workplace privacy regime to close the electronic surveillance gap.

Chapter 5 examines selected workplace privacy cases from Canada, the United States, and the European Union. There are two workplace privacy cases examined from each jurisdiction; each workplace privacy case is examined one by one. First, I thoroughly describe the workplace privacy case because an understanding of the background of employment cases is critical for conducting a sufficient analysis. Second, I analyze the case and note the principles and values that emerge from the analysis. The analysis contains a thorough examination of the workplace privacy cases that ties into the discussion various relevant social theory ideas involving surveillance and privacy. Third, I set out ideas for incorporating the detected principles and values into the proposed workplace privacy regime to close the electronic surveillance gap.

Chapter 6 has two main goals. First, it considers how the new proposed workplace privacy regime can be incorporated into the Canadian legal system. It examines the challenges involving the competing areas of law that are relevant to privacy, and

consequential jurisdictional issues in the Canadian federated system. It also sets out a plan for designing the new workplace privacy regime, and incorporates previous guidance provided by the Office of the Privacy Commissioner of Canada that is examined throughout the dissertation. Second, it provides some examples of proposed legislative provisions for the new workplace privacy regime. These examples are based on my ideas generated in Chapters 4 and 5.

Chapter 7 provides the Conclusion. It contains a brief review of what transpired during the dissertation, discusses limitations of the dissertation, and provides ideas for further research.

Chapter 2

2 Social Theory: Examination of Surveillance Theories

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live–did live, from habit that became instinct–in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.
>
> —George Orwell[98]

"Surveillance" comes from the French "*sur*", meaning "over", and "*veiller*", meaning "watch", and also from the Latin "*vigilare*", meaning "keep watch".[99] Together, the French term "*surveiller*" means "to watch, keep an eye on, or watch over".[100]

While dictionaries discuss watching over, many surveillance theorists agree that surveillance goes beyond watching because it depends on some capacity to control, regulate, or modulate behaviour.[101] For example, Torin Monahan and David Murakami Wood maintain that the term "surveillance" suggests that there is a power relationship involved, where there is some oversight that intervenes to shape behaviour.[102]

---

[98] George Orwell, *Nineteen Eighty-Four* (London: Penguin Books Ltd, 1990) at 4–5.
[99] Angus Stenson, ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010) *sub verbo* "surveillance".
[100] Charles Bimbenet, ed, *Collins LeRobert French Dictionary*, 10th ed (Glasgow: HarperCollins Publishers, 2016) *sub verbo* "*surveiller*".
[101] Torin Monahan & David Murakami Wood, "Introduction: Surveillance Studies as a Transdisciplinary Endeavor" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) ix at xix [Monahan & Wood, "Transdisciplinary Endeavor"].
[102] *Ibid.*

And while many associate surveillance with mass surveillance conducted by a State against its own citizens similar to what was revealed in 2013 by Edward Snowden,[103] ideas involving surveillance go beyond this conceptualization as well.

In fact, there is a rich body of theoretical work conducted by several surveillance theorists who attempt to understand surveillance. For example, an early surveillance theorist, James B. Rule, states that surveillance is about social control; it involves the mechanisms that discourage disobedience that either punishes such behaviour once it occurs, or prevents individuals with inclinations to disobedience from acting on those inclinations.[104] Rule notes that the workings of social control, especially efforts to impose or resist it, give rise to some of the most conflict-ridden chapters of social life.[105] He explains that this is why Orwell's *Nineteen Eighty-Four*[106] is so disturbing for many: "For the ugliest and most frightening thing about that world was its vision of total *control* of men's lives by a monolithic, authoritarian state".[107] The main goal is to enforce instant obedience.[108] Another example is David Lyon's definition of surveillance as the focused, systemic, and routine attention to personal details for purposes of influence, management, protection, or direction.[109] He states that surveillance, a normal part of everyday life, is both focused and systemic because attention to personal details is not random or spontaneous, but rather, deliberate and depending on certain protocols and techniques.[110] Lyon states that marketers wish to influence consumers, high schools attempt to manage students, and security companies wish to protect buildings; control is the common element, which may or may not involve malevolent intentions.[111]

---

[103] Edward Snowden, *Permanent Record* (New York: Metropolitan Books, 2019). Snowden disclosed information to the public relating to the mass surveillance by the National Security Agency (NSA) of citizens in the United States and abroad. Snowden worked as a contractor with the NSA in the role of systems administrator; some view him as a whistleblower, and others view him as a traitor.
[104] James B Rule, *Private Lives and Public Surveillance* (London: Penguin Books, 1973) at 20.
[105] *Ibid.*
[106] Orwell, *supra* note 98.
[107] Rule, *supra* note 104 at 19.
[108] *Ibid.*
[109] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007) at 14 [David Lyon, "Surveillance Studies"].
[110] *Ibid* at 14–15.
[111] *Ibid* at 15.

Monahan and Wood refer to surveillance studies as a transdisciplinary field given that surveillance theorists draw upon a wide range of sources and use different disciplinary perspectives to raise different concerns, methods, and theoretical positions to the study of surveillance in society.[112] A useful approach for understanding surveillance theories is to categorize them into specific topics and study the various approaches within categories that are most relevant to a particular research endeavor.[113]

To that end, the purpose of this Chapter is to examine the selected surveillance theories that are most relevant to this dissertation topic. I will focus on categories of theories that directly and indirectly relate to electronic surveillance in the employment context, both inside and outside the workplace. These categories of theories are not competing schools of theories, but are instead informative theories that can add to our knowledge of the nature and implications of electronic surveillance affecting the employment context from different angles. These theories form a foundation of instructive information concerning the sophisticated electronic surveillance technology for the purposes of creating the new workplace privacy regime.

If we picture a coin as the employment context, then ubiquitous surveillance and workplace surveillance are two sides of that same coin: ubiquitous surveillance theories are involved indirectly (outside the workplace), and workplace surveillance theories are involved directly (inside the workplace). If we imagine the rim of that coin running through and affecting both sides of that coin as the Panopticon (to be discussed below) we can view it as a vital component that touches on both ubiquitous and workplace surveillance theories. And if we step back and use a particular lens when examining this coin, that lens is the capitalist surveillance perspective of surveillance.

When using this lens, I stress throughout this Chapter that there are dangers associated with electronic surveillance. Surveillance capitalist theorists are relevant to electronic surveillance both inside and outside the workplace. These theorists draw on Karl Marx

---

[112] Monahan & Wood, "Transdisciplinary Endeavor", *supra* note 101 at xxi; David Lyon, "Surveillance Studies", *supra* note 109 at 48.
[113] Monahan & Wood, "Transdisciplinary Endeavor", *supra* note 101 at xxvi; David Lyon, "Surveillance Studies", *supra* note 109 at 48–49.

and use his ideas regarding managing human capital by way of the appropriation of the surplus value of labour through exploitation of the working class.[114] When applying these ideas to surveillance, we see that surveillance-based capitalism involves private-sector companies engaging in capital extraction of individuals' personal data to manipulate and control them by means of the exploitation of their personal information.[115] The theorists point out the dangers of ubiquitous surveillance as it relates to the general sphere outside employment, and also workplace monitoring as it relates to electronic surveillance inside the workplace. Many draw on panoptic concepts when aggressively warning against the dangers of the abuse of surveillance power. The Chapter highlights the consequences of this exploitation such as the panoptic sort, which involve dangerous outcomes involving discrimination and profiling. Ultimately, the perspective taken in this Chapter opposes the exploitation of individuals in the surveillance economy. And finally, it paves the way for Chapter 3 by criticizing surveillance theorists' views of privacy and arguing for the need to have individual privacy protections as conceptualized by privacy theorists.

2.1 The Beginning: The Panopticon

> La visibilité est un piège…Le Panopticon fonctionne comme une sorte de laboratoire de pouvoir.
>
> —Michel Foucault[116]

While the first notions of surveillance have been discovered in population documents from ancient Egypt and records of English landholding with the Domesday Book of 1086,[117] an effective starting point for studying surveillance issues is with the Panopticon,

---

[114] Monahan & Wood, "Political Economy", *supra* note 101, 281 at 281. See also Peter Kivisto, *Social Theory: Roots & Branches*, 5th ed (Oxford: Oxford University Press, 2013) at 3–38; Carsten Bagge Laustsen et al, *Social Theory: A Textbook* (London: Routledge, 2017) at 14−34, online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315657998>; Nick Dyer-Witheford, *Cyber-Proletariat: Global Labour in the Digital Vortex* (Toronto: Between the Lines, 2015) at 4−15, 19−38.
[115] Monahan & Wood, "Political Economy", *supra* note 101, 281 at 282−283.
[116] Michel Foucault, *Surveiller et Punir: Naissance de la Prison* (Paris: Gallimard, 1975) at 234, 238 [translation: "Visibility is a trap…The Panopticon functions as a kind of laboratory of power"] [Michel Foucault, "*Surveiller et Punir*"].
[117] Monahan & Wood, "Transdisciplinary Endeavor", *supra* note 101 at xxii.

the "all-seeing prison",[118] and Jeremy Bentham.[119] In fact, Bentham's early ideas about the Panopticon are referred to as a "touchstone of surveillance theory".[120]

To Bentham, while punishment is both evil and yet necessary for the common good, cruel punishment is unnecessary.[121] Bentham rejects the idea that by 1770, over 150 offences are punishable by death.[122] Therefore, Bentham's ideas regarding punishment involve milder punitive actions instead of the death penalty.[123] In fact, Bentham believes that perpetual imprisonment should take the place of death because it is more economical for the labour of criminals to benefit society, and because the idea of perpetual imprisonment holds more terror for criminals than extinction.[124]

Bentham describes the Panopticon as a beautiful and pleasant building, which he compares to a lantern and a glass bee-hive without a drone.[125] The structure is a circular or polygonal shape with cells around the circumference; the core has a central inspection area with galleries and a lodge that is disjoined from the main building and linked to the outer perimeter only by stairways.[126] From the lodge in the center inspection area, the watchers can carry out constant surveillance of the inmates while remaining invisible.[127] This center lodge is the focal point, and the central aperture must remain clear; the labyrinth of galleries, stairs, and passageways exist to separate and protect the warders from the inmates.[128] Architecturally, Bentham uses glass for skylights and two large windows in each cell, along with iron for pillars, arches, staircases, and galleries.[129]

---

[118] *Ibid* at 27.
[119] Jeremy Bentham was born in London in 1748. See Janet Semple, *Bentham's Prison: A Study of the Panopticon Penitentiary* (Oxford: Oxford University Press, 1993) at 20. Interestingly, the Panopticon was initially designed by Jeremy Bentham's brother, Samuel, as an efficient means of overseeing workers.
[120] Monahan & Wood, "Society and Subjectivity" in Monahan & Wood, *supra* note 101, 31 at 31 [Monahan & Wood, "Society and Subjectivity"].
[121] Semple, *supra* note 119 at 25–26.
[122] *Ibid* at 29.
[123] *Ibid.*
[124] *Ibid* at 30.
[125] *Ibid* at 114–116.
[126] *Ibid.*
[127] *Ibid.*
[128] *Ibid* at 119.
[129] *Ibid* at 116–117.

One important design goal of the Panopticon is to reverse the logic of the dungeon by spreading light and reason to the dark space where evil might flourish through illumination; by removing physical and moral evils, it is possible to reform and rehabilitate prisoners for the larger good.[130] So for Bentham, it is critical that the prisoners are stripped and washed upon arrival, constantly clean, and regularly shaven in order to remain morally pure.[131] The prisoners stay in a cell that is no larger than between nine and 13 feet deep and six feet wide, and at least nine feet in height.[132] The Panopticon is known for its paradox of "crowded solitude",[133] which is the chilling vision of human beings packed together, yet alone.[134] According to Bentham, labour can be converted to profit, even if combined with the expense of imprisonment.[135] Inmates of the Panopticon work 14 hours at sedentary labour each day.[136] Bentham refers to the Panopticon as "a mill for grinding rogues honest".[137] In addition to generating profits, work in the Panopticon leads to a significant reformation.[138]

Although Bentham ultimately rejects the idea of the Panopticon,[139] his ideas are later reconsidered and similarly rejected by an important surveillance theorist, Michel Foucault.[140]

Foucault examines Bentham's prison ideas and explores the Panopticon, where he notes the efficient control of individuals using the architecture of the building that allows for complete visibility of the individuals.[141]

---

[130] Monahan & Wood, "Society and Subjectivity", *supra* note 120 at 28.
[131] Semple, *supra* note 119 at 122.
[132] *Ibid* at 123.
[133] *Ibid* at 129.
[134] *Ibid*.
[135] *Ibid* at 27.
[136] *Ibid* at 125.
[137] *Ibid* at 152.
[138] *Ibid* at 155.
[139] *Ibid* at 166–191, 254–281.
[140] Michel Foucault was born in France in 1926. See Michel Foucault, *Power/Knowledge: Selected Interviews & Other Writings 1972–1977*, edited by Colin Gordon, translated by Colin Gordon et al (New York: Vintage Books, 1980) at 271 [Michel Foucault, "Power/Knowledge"].
[141] Monahan & Wood, "Society and Subjectivity", *supra* note 120 at 27.

Foucault states that it is more efficient and profitable, when considering the economy of power, to place people under surveillance than to subject them to some exemplary penalty.[142] In fact, he states that the prison is meant to be an instrument in a project of transformation that is comparable with and no less perfect than a school, barracks, or hospital.[143]

Foucault describes the architecture of the Panopticon as a building that is in the form of a ring, where the center has a tower that is pierced by large windows opening onto the inner face of the ring.[144] The outer building is divided into cells, each of which traverses the whole thickness of the building; each cell has two windows, one opening onto the inside that faces the central tower, and one opening to the outside that allows daylight to pass through the whole cell.[145] There is an overseer in the tower who watches the prisoners in the cells, and there is a backlighting in the cells that enables the overseer to pick out from the central tower silhouettes in the ring of cells.[146]

To Foucault, the combination of daylight, interiorization, and the overseer's gaze removes any protection a prisoner may have, increases visibility, and captures the inmate more effectively.[147] Indeed, he states that power is created through transparency.[148] Foucault notes that the inexpensive model involves using a simple gaze—there is no need for arms, physical violence, or material constraints.[149] He states:

> An inspecting gaze, a gaze which each individual under its weight will end by interiorizing to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost.[150]

---

[142] Michel Foucault, "Power/Knowledge", *supra* note 140 at 38.
[143] *Ibid* at 39–40.
[144] *Ibid* at 147.
[145] *Ibid.*
[146] *Ibid.*
[147] *Ibid.*
[148] *Ibid* at 154.
[149] *Ibid* at 155.
[150] *Ibid.*

According to Foucault, the illusion of power has considerable force, whereby individuals become virtuous by the simple fact of being observed.[151] Foucault discusses the relationship between discipline and "docile bodies".[152] He explains that a body is docile if it can be subjected, used, transformed, and improved.[153] He elaborates by outlining the methods (what he calls "disciplines"), which are typically general formulas of domination: scale of control (power over the active body); object of the control (the efficiency of movements and their internal organization); and the modality (an uninterrupted, constant coercion, supervising the processes of the activity rather than its results).[154] He maintains that, while discipline produces docile bodies, the manipulation of the body, its gestures, and its behaviour creates a mechanics of power.[155] What is more, he contends that discipline dissociates power from the body, turns it into an aptitude and capacity, and creates a relation of strict subjection.[156]

Foucault also explores ideas involving using disciplinary power as a way to train individuals such that, "Discipline 'makes' individuals; it is the specific technique of power that regards individuals both as objects and instruments of its exercise".[157] He considers hierarchized, continuous, and functional surveillance and states that it, "may not be one of the great technical 'inventions' of the eighteenth century, but its insidious extension owed its importance to the mechanisms of power that it brought with it".[158] He notes that the power in hierarchical surveillance functions like a piece of machinery.[159] He states:

> This enables the disciplinary power to be both absolutely indiscreet, since it is everywhere and always alert, since by its very principle it leaves no zone of shade and constantly supervises the very individuals who are entrusted with the task of supervising; and absolutely 'discreet', for it functions

---

[151] *Ibid* at 161.
[152] Michel Foucault, *Discipline & Punish: The Birth of the Prison*, 2nd ed, translated by Alan Sheridan (New York: Vintage Books, 1995) at 135–169 [Michel Foucault, "Discipline & Punish"].
[153] *Ibid* at 136.
[154] *Ibid* at 137.
[155] *Ibid* at 138.
[156] *Ibid.*
[157] *Ibid* at 170.
[158] *Ibid* at 176.
[159] *Ibid* at 177.

> permanently and largely in silence. Discipline makes possible the operation of a relational power that sustains itself by its own mechanism and which, for the spectacle of public events, substitutes the uninterrupted play of calculated gazes.[160]

Foucault asserts that disciplinary power is exercised through its invisibility—at the same time, it imposes on those whom it subjects a principle of compulsory visibility.[161] In particular, visibility maintains the hold of the power that is exercised over the subjects.[162] He curtly states, "Visibility is a trap".[163] Another important element for Foucault when describing the Panopticon is ensuring that inmates never know whether they are being watched at any one moment, so they must be sure that they may always be watched.[164] In fact, since anyone could be watching, there is a greater risk that the inmate will be anxious about being continuously watched by anonymous observers.[165] What is visible is the constant tall outline of the central tower from which the individual is spied on; what is invisible is the not knowing whether the individual is actually being watched at any one moment.[166]

While the architecture of the Panopticon is fascinating, there is no question that the design is extremely manipulative. Foucault notes that the goal is to trap individuals using compulsory visibility, and to create anxiety among inmates so they are constantly worried about being watched by anonymous, invisible observers. The result is that the subjects self-censor and change their behaviour to become obedient. It is not surprising that Foucault describes the Panopticon as a "marvelous machine which, whatever use one may put it to, produces homogenous effects of power".[167]

What is most disturbing is that, when Foucault describes the Panopticon, he states that it can be used as a laboratory to carry out experiments and monitor their effects; for example, one can manipulate different punishments for different prisoners and then study

---

[160] *Ibid.*
[161] *Ibid* at 187.
[162] *Ibid.*
[163] *Ibid* at 200.
[164] *Ibid* at 201.
[165] *Ibid* at 201−202.
[166] *Ibid* at 201.
[167] *Ibid* at 202.

the effects.[168] He goes so far as to say that the Panopticon is "a privileged place for experiments on men".[169] What is more, Foucault states:

> The Panopticon functions as a kind of laboratory of power. Thanks to its mechanisms of observation, it gains in efficiency and in the ability to penetrate into men's behaviour; knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised.[170]

Foucault also points out that the productive increase of power can be assured only if it is exercised continuously in the very foundations of society, in the subtlest possible way.[171] There is only one way to describe the panoptic schema aimed at perfecting the exercise of power[172]—devious and unscrupulous.

Foucault states that what he describes as a "circular cage"[173] is a great failure of penal justice since prisons do not diminish the crime rate; he accepts that detention causes recidivism.[174] More specifically, Foucault notes that prisons may be multiplied or transformed, but still, the quantity of crime and criminals remains stable or even increases.[175] Further, those who leave prison have more chance than before of returning to it—convicts are in very high proportion former inmates.[176] He states that prisons cannot fail to produce delinquents, and they make it possible and even encourage the organization of delinquents who are commit future criminal acts.[177] He adds that conditions to which free inmates are subjected, including surveillance by police, create a situation where recidivism is more likely.[178] To this, he encourages the use of the seven universal maxims of the good "penitential condition".[179] He argues that delinquency is

---

[168] *Ibid* at 203–204.
[169] *Ibid* at 204.
[170] *Ibid*.
[171] *Ibid* at 208.
[172] *Ibid* at 206, 208.
[173] *Ibid* at 208.
[174] *Ibid* at 264−265.
[175] *Ibid* at 265.
[176] *Ibid*.
[177] *Ibid* at 266−267.
[178] *Ibid* at 267.
[179] *Ibid* at 269−270 These principles involve: the essential function of transformation of behaviour; isolation depends on the gravity of the act, age, mental attitude, correction techniques, and stages of transformation; altering penalties according to individuality of convicts, results, progress or relapses; a

one result of the system, but it also becomes part of and an instrument of it—it forms part of a circuit that is never interrupted: "police surveillance provides the prison with offenders, which the prison transforms into delinquents, the targets and auxiliaries of police supervisions, which regularly send back a certain number of them to prison."[180]

There is no doubt that the design of the Panopticon is troubling in that it has a strong potential to create an exploitive abuse of surveillance power in order to control individuals. Given that this type of disciplinary power creates mechanisms of power that facilitate a relation of strict subjection, there is no attempt to preserve any sense of self-determination among the inmates. Likewise, there is no attempt to treat the inmates as real people because they are simply viewed as pawns that are used in a game of manipulation. Indeed, Janet Semple characterizes the concept of ceaseless invisible inspection as profoundly disturbing, stating:

> The Panopticon can too easily become the prototype of a fiendishly efficient instrument of totalitarian control, of ruthless social engineering, and psychological manipulation. It has been deployed by his philosophic adversaries to suggest that the whole of Benthamite political theory is authoritarian and repressive…And for Michel Foucault, the Panopticon is a cruel and ingenious mechanism of the new physics of power designed to subjugate the individual.[181]

In sum, I have explained the Panopticon as initially envisioned by Bentham, including its architectural design and Bentham's goals to replace the death penalty with milder forms of punitive action. I then discussed how Foucault views the Panopticon, and how he examines the combination of daylight, interiorization, and the overseer's gaze for the purposes of increasing visibility. I also noted the dangers of the Panopticon and its potential to dominate and control through an abuse of surveillance power. It was

---

focus on transformation and progressive socialization of convicts; education of the prisoner; supervision of the regime by a specialized staff with moral qualities and technical abilities; and imprisonment followed by rehabilitation and supervision.

[180] *Ibid* at 282.

[181] Semple, *supra* note 119 at 316.

important to study the Panopticon since the abuse of panoptic power applies both inside and outside the workplace.

I will now turn to the issues involving ubiquitous surveillance—this is important since it is the first side of the coin that involves activities that take place outside the workplace that can affect the employment context.

2.2 The Dangers of Ubiquitous Surveillance

In this part I will discuss the nature of ubiquitous surveillance, and also the dangers associated with it. These dangers are relevant because what is discovered outside the workplace can affect what happens inside the workplace.

Today's surveillance theorists acknowledge that surveillance is ubiquitous in modern times; for instance, David Lyon maintains that systemic, routine, everyday surveillance has rapidly multiplied.[182]

Roger Clarke and Graham Greenleaf define the ever-growing concept of dataveillance as "the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons".[183] Dataveillance can involve surveillance of an individual (defined as the surveillance of an identified person of interest for a specific reason) or mass surveillance (defined as the surveillance of groups of people to identify individuals who belong to a class of interest).[184] They discuss the underlying concept of the "digital persona", which is an individual's public personality based on data and maintained by transactions; this digital persona is used as a proxy for the individual.[185]

Gavin Smith elaborates on the concept of a "data-proxy", and explains that exhaust, or data trails, give rise to "an abstracted figure created from the amalgamation of data traces

---

[182] David Lyon, "Surveillance Studies", *supra* note 109 at 181.
[183] Roger Clarke & Graham Greenleaf, "Dataveillance Regulation: A Research Framework" (2017) 25:1 J L Info & Sci 104 at 105, 108.
[184] *Ibid* at 105.
[185] *Ibid* at 106.

which serves as a representational signifier of selfhood in networked transactions between social actors and audiences".[186] Moreover, he states that data-proxies paint virtual portraits of a person's habits and situation, like a networked impression of self for the purposes of establishing positive social relations and identity.[187] Further, individuals aim to project a successful networked profile in order to avoid suffering data-derived harm and to enhance autonomy.[188]

Clarke and Greenleaf believe that the purpose of dataveillance is to watch the shadow of a person that is cast as that person conducts economic, social, or political transactions.[189] They contend that dataveillance is conducted by using several techniques, some of which include profiling, data matching, and the monitoring of search terms.[190] They also explain that a full understanding of any instance of surveillance requires that it is considered with respect to four temporal dimensions: the timeframe in which the surveillance is conducted (ephemeral, across a single span of time, across recurrent spans such as within 24-hour cycles, or scattered across time following a trigger); the intensity with which surveillance is conducted (once, repeated, or continuous); the persistence of consequences of surveillance (ephemeral because it is limited to observation, short-to-medium term because it is recorded, or long-term or permanent because it is archived); and the time period within which surveillance is applied (the present, real-time use, the past through retrospective use, or the future through prospective or predictive use).[191]

Clarke and Greenleaf describe several forms of surveillance that have electronic features, such as: physical observation accompanied with audio or video streaming to another location; communications surveillance which can include metadata about the messages; location surveillance which can be caught in logs of vehicle movements; experience surveillance noting patterns of behaviour which can be captured on CCTV images or with

---

[186] Gavin JD Smith, "Surveillance, Data and Embodiment: On the Work of Being Watched" (2016) 22:2 Body & Society 108 at 110, online (pdf): *SAGE Publishing* <bod.sagepub.com> DOI: <10.1177/1357034X15623622>.
[187] *Ibid* at 110–111.
[188] *Ibid* at 119.
[189] Clarke & Greenleaf, *supra* note 183 at 106.
[190] *Ibid.*
[191] *Ibid* at 108–109.

lists of search terms; and bodily surveillance including biometrics used with streaming to another location.[192]

To recap for a moment, I have noted that there are several theorists such as Lyon, Clarke and Greenleaf, and Smith, who provide a foundation of understanding regarding the nature of electronic surveillance and the digital persona involving ubiquitous surveillance.

But other theorists more adamantly point out some of the dangers associated with ubiquitous surveillance. For instance, Mark Andrejevic contemplates automated data collection and processing, and argues that surveillance goes beyond what even Foucault imagined with the internalization of the monitoring gaze; automated surveillance replaces deterrence by simply predicting and pre-empting.[193] The "always-on" monitoring that enables predictions requires digital infrastructures and platforms, and most importantly, automation.[194] Automation is a critical feature because large quantities of information are generated using embedded sensors, and this can only be accomplished technically with automated data processing.[195]

Though the technology is intriguing, Andrejevic insists our dependence on digital media, together with the omnipresent monitoring, can lead to unwanted consequences:

> We are rapidly headed toward a world in which all aspects of our lives become increasingly dependent upon digital media that, in turn, create comprehensive records of our activities, communications, purchases, and—to the extent that these can be rendered in digital form—our thoughts, hopes, and dreams.[196]

Andrejevic points to the dangers and asserts that ubiquitous surveillance creates a potential for exploitation of individuals through the abuse of surveillance power, stating:

---

[192] *Ibid* at 109–110.
[193] Mark Andrejevic, "Automating Surveillance" (2019) 17:1/2 Surveillance & Society 7 at 10, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> [Mark Andrejevic, "Automating Surveillance"].
[194] *Ibid* at 7.
[195] *Ibid* at 8.
[196] *Ibid* at 7.

> When we speak of surveillance, we also typically invoke asymmetrical power relations between watcher and watched, with the former in the dominant position.[197]

He notes that, while there are several benefits associated with recent technological development associated with ubiquitous monitoring, there is also an accompanying deep-seated social anxiety: "that we all fundamentally depend on forms of trust that can be abused and disappointed".[198] Andrejevic states that the necessary forms of trust built into our daily lives and our dependence on them have become a "vector of vulnerability".[199]

Most importantly, however, Andrejevic posits that the endpoint of data-driven decision-making is the automation of judgment.[200] He identifies a serious problem: the idea of mechanic neutrality is not possible given the incomplete, inaccurate, or biased data and algorithms that are crafted by humans using human limitations—this occurs when we attempt to clean the data, make it accurate, and turn the development of automated systems over to the machines themselves.[201] Ultimately, Andrejevic concludes that we are developing systems that replace societal decisions governing life, liberty, and opportunity.[202]

Moreover, Andrejevic considers big data surveillance, and states that the strategy has recently transformed from starting with a suspect to monitor due to suspicion, to starting with generalized surveillance and subsequently generating suspects.[203] That is, using surveillance and simulations, the strategy is to intervene in the future by modeling it.[204] Andrejevic explains that data mining and profiling involves managing information and communications, and subsequently using control mechanisms by forecasting all

---

[197] *Ibid.*
[198] *Ibid* at 9.
[199] *Ibid.*
[200] *Ibid* at 12.
[201] *Ibid.*
[202] *Ibid.*
[203] Mark Andrejevic, "Surveillance in the Big Data Era" in Kenneth D Pimple, ed, *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards* (New York: Springer, 2014) 55 at 58 [Mark Andrejevic, "Big Data Era"].
[204] *Ibid.*

conceivable outcomes in advance.[205] In order to accomplish this goal, it is necessary to have comprehensive monitoring, which is also known as ubiquitous surveillance.[206] He says that to model the future and then modulate the present to intervene in it, several elements must be present: tracking everyone in the group; studying correlations for revealing predictability; monitoring in a pre-emptive manner so that outcomes are not only predicted but also altered; ensuring that the tracking is interventionist in that there can be forms of experimentation to generate even more data; collecting all information because it is relevant; and tracking anonymously because the goal is to detect patterns of correlations (however, he admits that some tracking leads to individuals being identified simply by scraping data off the Internet).[207]

Andrejevic reflects on the ethics of big data and pervasive surveillance, and argues that data becomes a form of power when it is used to manipulate individuals and to shape the information that is available to them.[208] He contends that this is particularly concerning when dealing with the level of influence, the categorization of individuals, and consequent decision-making.[209] Similarly, he notes the dangers associated with "function creep", which is the repurposing of personal information for new uses, other than those for which the information was originally collected, so that additional purposes are created unbeknownst to the data subject.[210]

I have just noted Andrejevic's concerns about this powerful and complicated technology. But the next few theorists stress that we are exposing ourselves when we participate in our own surveillance—making the situation worse.

For example, Colin J Bennett, Kevin D. Haggerty, David Lyon, and Valerie Steeves state that opportunities to conduct ubiquitous surveillance have expanded because of our new digital existence and also because of the increased sophistication of surveillance

---

[205] *Ibid.*
[206] *Ibid.*
[207] *Ibid* at 58–65
[208] *Ibid* at 65–67.
[209] *Ibid.*
[210] *Ibid* at 67–68.

systems.[211] They highlight that we encounter surveillance everywhere—in our cars, buildings, and homes.[212] Moreover, Bennett et al note that social media use and mobile devices have created an explosion of possibilities to monitor individuals.[213] We watch each other; it can be playful to be watched and to watch others, to stay connected with people, and to engage in activities such as posting content, tagging photos, and liking pictures or videos.[214] However, they emphasize that every time we post personal information online, we inadvertently participate in our own surveillance because information can be easily captured by anyone, ranging from marketers, stalkers, the State, employers, or identity thieves, who use the information for their own purposes.[215] What is dismaying is that surveillance conducted by organizations involves the more powerful governments, employers, and businesses watching the less powerful.[216] Bennett et al. state:

> The contemporary expansion of surveillance, such that monitoring becomes an ever more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger in all of this is therefore not that a specific surveillance measure will be too intrusive, or that mistakes will be made in identifying or processing people, or that data will be lost. Instead, the most significant—but impossible to quantify—danger comes from the simple fact that we are creating, step by step, a society that is hard-wired for surveillance and that such devices can easily be turned to oppressive uses.[217]

Perhaps this is why Andrejevic asserts that individuals are creating their own digital enclosures; he suggests that the exploitation involved with being constantly watched has created a situation where there is a shift in control over personal information from individuals to private corporations.[218] Also disconcerting is that he states that, for the

---

[211] Colin J Bennett et al, *Transparent Lives: Surveillance in Canada* (Edmonton: AU Press, Athabasca University, 2014) at viii–ix, 19 [Bennett et al, "Transparent Lives"].
[212] *Ibid* at ix.
[213] *Ibid.*
[214] *Ibid* at 167–170.
[215] *Ibid* at 170–171.
[216] *Ibid* at 168, 179.
[217] *Ibid* at 36.
[218] Mark Andrejevic, "The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure" (2002) 19:2 Critical Studies in Media Communication 230 at 237–239, 243–244, online (pdf): *tandfonline* <https://www.tandfonline.com> DOI: 10.1080/07393180216561 [Mark Andrejevic, "Being Watched"].

sake of creating a customized experience, individuals provide various details such as behavioural habits and consumption preferences.[219]

Indeed, Lyon argues that we live in a surveillance society and exist in a culture of surveillance whereby our daily lives are recorded, monitored, and tracked in unprecedented ways—everyday life routines play an increasing role in constituting surveillance through interactivity and user-generated surveillance, to the point where surveillance has become part of a way of seeing and being in the world.[220] He opines that it is hard if not impossible not to participate in the culture of surveillance.[221] In fact, he asserts that corporations are involved in extensive surveillance, and perhaps even more so than State agencies, because they do so in less obvious ways; as a result, surveillance is taken for granted and ultimately becomes a less perceptible "part of the furniture".[222]

Likewise, Bernard E. Harcourt emphasizes that we live in an expository society:

> In our digital frenzy to share snapshots and updates, to text and video chat with friends and lovers, to "quantify" ourselves, we are exposing ourselves —rendering ourselves virtually transparent to anyone with rudimentary technological capabilities. We are exhibiting ourselves through petabytes of electronic traces that we leave everywhere, traces that can be collected, linked together, and amalgamated, traces that paradoxically, although they are virtual, have become more tangible, more provable, more demonstrable, and more fixed than our analog selves.[223]

Harcourt warns that by exposing ourselves in this way, we make it easy, tempting, and cheap to watch us, monitor us, target us, track us, detain us, and for some, to extract and punish us—we allow ourselves to be shaped in unprecedented ways, intentionally or unwittingly.[224] He asserts that our new social condition is radically transforming our relations to each other, our community, and ourselves.[225] What is most troubling is that

---

[219] *Ibid.*
[220] David Lyon, *The Culture of Surveillance* (Cambridge: Polity Press, 2018) at 30 [David Lyon, "Culture of Surveillance"].
[221] *Ibid* at 54.
[222] *Ibid* at 83.
[223] Bernard E Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015) at 13.
[224] *Ibid* at 14.
[225] *Ibid* at 15.

he cautions that we are no longer being coerced; we are exposing or exhibiting ourselves knowingly with love, lust, passion, and politics.[226]

Even though we seem to understand that there are dangers, Lyon states that we still give up our personal information freely and fully, and voluntarily participate in the surveillance culture through our regular social media activity.[227] We continue to engage in social networking sites because it is fun and entertaining—a phenomenon referred to as the "privacy paradox".[228] Susan B. Barnes notes that we reveal intimate thoughts and behaviours online, while at the same time, government agencies and marketers are collecting personal data about us.[229] As articulated by Alyson Leigh Young and Anabel Quan-Haase, the privacy paradox is the willingness to disclose personal information on social network sites, despite expressing high levels of concern about privacy.[230]

To this point, I have discussed how theorists such as Bennett et al., Lyon, Harcourt, Susan B. Barnes, as well as Alyson Leigh Young and Anabel Quan-Haase stress that we regularly encounter ubiquitous surveillance, and we are aggravating the situation by willingly exposing ourselves and putting ourselves at risk for mistreatment.

Still, other theorists more aggressively point out that we are being exploited by capital in a surveillance economy.

More specifically, Nicole S. Cohen alerts us that social networking companies capitalize on time spent participating in communicative activity and information sharing; she states that producer-consumers (prosumers) provide the content to generate the traffic, and the companies leverage this content into advertising sales.[231] For example, Facebook

---

[226] *Ibid* at 18.
[227] David Lyon, "Culture of Surveillance", *supra* note 220 at 115–117.
[228] *Ibid.*
[229] Susan B Barnes, "A Privacy Paradox: Social Networking in the United States" (2006) 11:9 First Monday, online: *First Monday* <https://firstmonday.org> DOI: 10.5210/fm.v11i9.1394.
[230] Alyson Leigh Young & Anabel Quan-Haase, "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited" (2013) 16:4 Information, Communication & Society 479 at 479−481, online (pdf): *Taylor & Francis* <www-tandfonline-com> DOI: 10.1080/1369118X.2013.777757 [Young & Quan-Haase, "Privacy Protections"].
[231] Nicole S Cohen, "The Valorization of Surveillance: Towards a Political Economy of Facebook" in Monahan & Wood, *supra* note 101, 298 at 298.

capitalizes on the productivity of community members by using surveillance.[232] Cohen shares the unsettling fact that, as the community members are enjoying the social features provided by the company, these companies "obscure economic relations that reflect larger patterns of capitalist development in the digital age".[233]

But Christian Fuchs goes further than this. He discusses the growing phenomenon of the progressive blurring of the line separating producers and consumers, as these prosumers engage in "prosumption" when they generate online content.[234] He warns that the combination of surveillance and prosumption is at the heart of capital accumulation on web 2.0—the surveillance conducted on individuals and groups is aimed at controlling behaviour because they know that their appearance, movements, location, or ideas could be watched by surveillance systems.[235] He urges that ultimately, users produce surplus value and are largely exploited by capital; companies like Google and Facebook exploit the surplus value while providing free access to the services and platforms so users can continue to produce the content.[236] This is especially common in scenarios involving entertainment, play, and fun.[237] Fuchs boldly claims that:

> Surveillance is a specific kind of information gathering, storage, processing and assessment, and its use involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation, domination and disciplinary power. It is an instrument and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals. It tries to bring about or prevent certain behaviours of groups or individuals by gathering, storing, processing, diffusing, assessing and using data so that potential or actual physical, ideological or structural violence can be directed against humans in order to control and steer their behaviour.[238]

---

[232] *Ibid.*
[233] *Ibid.*
[234] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" in Monahan & Wood, *supra* note 101, 276 at 277 [Christian Fuchs, "Web 2.0"].
[235] *Ibid* at 276–277 [Christian Fuchs, "Web 2.0"].
[236] *Ibid* at 277.
[237] *Ibid* at 279.
[238] Christian Fuchs, "Political Economy and Surveillance Theory" (2012) 39:5 Crit Sociology 671 at 685, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1177/0896920511435710> [Christian Fuchs, "Political Economy"].

One of the most dynamic and persuasive capitalist surveillance theorists to highlight concerns about the abuse of surveillance power, Shoshana Zuboff, continues and goes even further when she vigorously stresses that a new form of information capitalism aims to predict and modify human behaviour to produce revenue and market control.[239] She explains that big data comes from: data from computer-mediated economic transactions with companies; data from billions of sensors embedded in several objects, bodies, and places such as wearables; data from corporate and government databases such as banks or credit card companies; and surveillance cameras that are private or public such as Google Street View.[240] She points to the distressing fact that large tech companies such as Google have engaged in data extraction and exploitation through monitoring efforts and creating profiles.[241] She states:

> Surveillance capitalism establishes a new form of power in which contract and the rule of law are supplanted by the rewards and punishments of a new kind of invisible hand.[242]

Zuboff unapologetically insists that surveillance capitalism has become a new breed of economic power in which every casual search, like, and click is claimed as an asset to be tracked, parsed and monetized by a large tech company.[243] Zuboff reminds us that in this world, netizens are neither customers nor products; they are sources of raw material supply (behavioural data surplus) in a raw material extraction operation, and the products are about predicting individuals' future behaviour without caring about them at all.[244] She cautions that the goal of the main Internet companies is to assess behavioural data and subsequently know what a particular individual is thinking, feeling, and doing at any moment in time in any place.[245] Zuboff states:

---

[239] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30 Journal of Information Technology 75 at 75–76, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1057/jit.2015.5> [Shoshana Zuboff, "Big Other"].
[240] *Ibid* at 78.
[241] *Ibid* at 78–82.
[242] *Ibid* at 82.
[243] Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019) at 52–53 [Shoshana Zuboff, "Surveillance Capitalism"].
[244] *Ibid* at 10, 69–70.
[245] *Ibid* at 69–70.

> That this no longer seems astonishing to us, or perhaps even worthy of note, is evidence of the profound psychic numbing that has inured us to a bold and unprecedented shift in capitalist methods.[246]

In fact, Zuboff goes so far as to say that companies such as Google use additional data from services such as Google Search to create new capabilities to infer and deduce the thoughts, feelings, intentions, and interests of individuals and groups with an automated architecture that operates as a one-way mirror irrespective of one's awareness, knowledge, and consent; this enables privileged secret access to behavioural data, and subsequently, these raw materials transform into surveillance capital.[247] She explains the process of discovering behavioural surplus as follows:

> Surveillance capitalism begins with the discovery of behavioral surplus. More behavioral data are rendered than required for service improvements. This surplus feeds machine intelligence – the new means of production – that fabricates predictions of user behaviour. These products are sold to business customers in new behavioral futures markets.[248]

What is most concerning is that Zuboff uncovers the attitudes of the main Internet companies who aim to avoid government regulation and the voicing of privacy concerns.[249] Zuboff insists that surveillance capitalists are impelled to pursue lawlessness by the logic of their own creation:

> Google and Facebook vigorously lobby to kill online privacy protection, limit regulations, weaken or block privacy-enhancing legislation, and thwart every attempt to circumscribe their practices because such laws are existential threats to the frictionless flow of behavioral surplus.[250]

Zuboff provides an example of the danger of having no checks in place: Internet companies can easily exploit their powers, such as with the Google Street View operation (pictures were taken on the ground to organize the world's information) consisting of a covert data sweep, secretly collecting personal information from private Wi-Fi networks in people's homes, where stolen personal information included names, telephone numbers, credit information, passwords, messages, emails, chat transcripts, records of

---

[246] *Ibid* at 78.
[247] *Ibid* at 80–81, 94.
[248] *Ibid* at 97.
[249] *Ibid* at 105.
[250] *Ibid*.

online dating, pornography, browsing behaviour, medical information, location data, photos, along with audio and video files—enough information to create data packets that could be assembled to form a detailed profile of an identifiable person.[251]

Zuboff's main concern here is inevitabilism, a situation where no room is left for humans to believe that they have free will and that they are the authors of their futures.[252] In short, she is concerned that humans will not be able to be allowed to enjoy the right of self-determination. One example that raises several questions is the Google City in connection with Sidewalk Labs, where all smart devices are connected, collecting and sharing behavioural data—Zuboff asks what a smart product knows, who it tells, who knows the information, who makes decisions, and who decides the actors who make these decisions.[253] What is most alarming with respect to these smart devices and applications is the absence of meaningful privacy policies.[254]

Also unsettling, Zuboff sheds light on the goal of large Internet companies: to be able to accurately predict behaviour after rendering the data.[255] And, not only is the goal to predict behaviour, but it is also to shape behaviour by modifying real-time actions in the real world since connected smart sensors can register and analyze any kind of behaviour and determine how to manipulate it by using nudges (tuning), controlling a person's context (herding), and mastering schedules of reinforcement (conditioning).[256] These strategies are based on learning theories by behaviourists such as Watson, Pavlov, and Skinner.[257] Zuboff warns that the end goal is to automate information flows about people to automate people for the purposes of modification, prediction, monetization, and control.[258] She suggests that the ultimate goal is to create a collective, where behaviour is carried out for the greater good, and where there is social pressure for harmony through

---

[251] *Ibid* at 143–144.
[252] *Ibid* at 227.
[253] *Ibid* at 227–232, 238.
[254] *Ibid* at 251.
[255] *Ibid* at 275.
[256] *Ibid* at 293–296.
[257] *Ibid* at 296.
[258] *Ibid* at 339–340, 352.

the use of social physics and the weakening of individuality.[259] To that end, Zuboff insists that there needs to be a freedom of will and a right to the future tense for us to live a fully human life.[260] What she is arguing for then, in other words, is a right to be treated as a human being with self-determination and autonomy in the midst of endless corporate attempts to continuously monitor and control behaviour for their own benefit.

Let me pause here for a moment. I have discussed several theories regarding the nature and the associated dangers of ubiquitous surveillance. I just emphasized the views of the most assertive and convincing theorists such as N. Cohen, Fuchs, and Zuboff, when it comes to the exploitation of users in the surveillance economy.

I will now focus on some of the consequences that arise due to the abuse of surveillance power in this regard.

More precisely, social surveillance in the ubiquitous realm creates a potential for discriminatory practices. Oscar H. Gandy, Jr. refers to the "panoptic sort"[261] to describe a system of social control where the State and corporate bureaucracies collect, process, and share massive amounts of personal information to track, command, coordinate, and control individuals to an unimaginable extent.[262] He stresses that the panoptic sort is "a kind of high tech cybernetic triage through which individuals and groups of people are sorted according to their presumed economic or political value" and insists that the poorer classes of individuals, especially minorities, are "increasingly being treated as broken material or damaged goods to be discarded or sold at bargain prices to scavengers in the marketplace".[263]

In fact, Gandy Jr. cautions that this sorting mechanism only exacerbates the massive and destructive inequality that characterizes the political economy as it moves forward into

---

[259] *Ibid* at ch 15–16.
[260] *Ibid* at 332, ch 17–18.
[261] Oscar H Gandy, Jr, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, Co: Westview Press, 1993) at 1 [Gandy, Jr, "The Panoptic Sort"].
[262] *Ibid*.
[263] *Ibid* at 1–2.

the information age.[264] He notes that the panoptic sort increases the ability to organize interests and communicate differentially with individuals to influence behaviour.[265] And he asserts that the panoptic sort is a technology that is continually revised to serve the interests of the decision makers within both government and corporate bureaucracies.[266] Gandy Jr. warns that, although corporations need accurate and timely information for the purposes of efficiency of their production process, strategic planning, and making analytical models of performance and potential, the quality of information is suspect and susceptible to errors of measuring, misinterpretation, and strategic modification such that the analysis only becomes more flawed with compounding errors.[267]

Gandy Jr. states that the information that is collected, processed, and shared is generated through the daily lives of citizens, employees and consumers.[268] He argues that the panoptic sort is a system of disciplinary surveillance that sorts individuals into categories and classes on the basis of their routine measurements; in this way, it is discriminatory since it allocates options and opportunities on the basis of those measures and the administrative models that they inform.[269]

What is more, Gandy Jr. states that inequality is inherent in situations where individuals are dealing with organizations; the power that individuals exercise over the organization when they withhold personal information is almost always insignificant, compared with the power of the organization that chooses to withhold goods or services unless information is provided.[270] Gandy Jr. explains that prediction is of central importance to the panoptic sort for forecasting outcomes that are likely for classes of individuals; this is important because predictability reduces uncertainty about individual behaviour, and the use of power can induce a desired and predictable reaction.[271] He suggests that the heart

---

[264] *Ibid* at 2.
[265] *Ibid.*
[266] *Ibid* at 95.
[267] *Ibid* at 60–61.
[268] *Ibid* at 15.
[269] *Ibid.*
[270] *Ibid* at 19.
[271] *Ibid* at 45.

of the panoptic sort is the pursuit of improvement of predictability.[272] Gandy Jr. states that, "The panoptic sort is a system of power".[273]

As a result, we see such things as racial profiling, which Gandy Jr. describes as, "a low-level form of predictive technology".[274] For example, with respect to the discriminatory consequences of sorting in the criminal justice system, while criminal profiles used by police typically contain several characteristics in the analysis, he says that racial profiles collapse the entire set of characteristics and place a greater weight on the race of the individual.[275] Gandy Jr. explains that the reason this is troubling is because many of the analytical models contain indicators or variables that are biased.[276] For instance, Gandy Jr. stresses that authority acts on the assumption that African Americans are more likely to be engaged in criminal behaviour; this translates into more stops, searches, and arrests.[277] As a result, African Americans are on average subject to significantly more extensive policing, and this affects the quality of the relationship between the parties.[278]

In addition to racial profiling, there are other groups who experience differential treatment as a result of surveillance and panoptic sorting; for example, feminist surveillance scholars, Corinne Mason and Shoshana Magnet, note the history of inequality associated with surveillance practices, especially stalking and violence against women.[279] They define stalking as obsessive behaviour directed toward another person involving persistent, malicious, and unwanted surveillance that is seen as a constant threat to the victim's personal security.[280] Mason and Magnet explain that electronic technologies can be used by abusers to monitor the actions and movements of victims;

---

[272] *Ibid.*
[273] *Ibid* at 15.
[274] Oscar H Gandy, Jr, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage* (Surrey: Ashgate, 2009) at 124 [Gandy, Jr, "Chance"].
[275] *Ibid*.
[276] *Ibid.*
[277] *Ibid.*
[278] *Ibid* at 126.
[279] Corinne Mason & Shoshana Magnet, "Surveillance Studies and Violence Against Women" (2012) 10:2 Surveillance & Society 105 at 106–107, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> [Mason & Magnet, "Surveillance Studies and Violence"].
[280] *Ibid* at 107.

some of these technologies that can be used to harass and track targets include GPS, electronic records, Internet search engines, text messages, and social media.[281] Another unsettling consequence of using electronic surveillance is the use of spyware to monitor online activities of targets and learn the locations of crisis centers and shelters.[282] Mason and Magnet emphasize that surveillance technologies reflect the cultural context which is filled with persistent inequalities and the perpetuation of violence against women.[283]

I have therefore examined issues involving ubiquitous surveillance, and this was important since it was the first side of the coin involving activities that take place outside the workplace that can affect the employment context. As noted above, the dangers discussed have undesired consequences such as discrimination and violence as noted by Gandy Jr. and Mason and Magnet respectively.

I will now turn my attention to the other side of the coin—the theories that deal with electronic surveillance inside the workplace.

2.3 The Struggles Regarding Surveillance in the Workplace

In this part I will discuss the nature of surveillance that is conducted inside the workplace, and also the dangers associated with it. As will be seen below, this part explores the impact of electronic surveillance in employment relationships characterized by power imbalances, and notes the effects on employee trust in management.

Kirstie Ball provides significant insights into the area of electronic surveillance and monitoring of employees in organizations. She provides a solid foundation for understanding the nature of electronic surveillance that arises in the workplace. Ball states that surveillance in the workplace refers to management's ability to monitor, record, and track employee performance, behaviours, and personal characteristics in real

---

[281] *Ibid.*
[282] *Ibid* at 108.
[283] *Ibid* at 116.

time or as part of broader organizational processes.[284] Ball explains that surveillance generally functions as a way of controlling access to different levels of the organizational hierarchy and to the organization itself.[285] She notes that information is collected on employees using surveillance with a range of techniques from computer and telephone logging, to CCTV, to mobility tracking, to electronic recruitment.[286] She attributes the increase in employee monitoring to the Internet, and notes that it is very common for companies to monitor worker communications and on-the-job activities.[287] She also states that surveillance techniques are rarely the subject of collective bargaining.[288]

Ball simply accepts that workplace surveillance and business organizations go hand-in-hand and employee monitoring is nothing new.[289] To support this point, she cites older types of surveillance such as clocking-in or counting and weighing output for payment by piece-rate.[290] Nevertheless, she then admits that business organizations are hierarchies that function by superordinate positions monitoring and controlling positions below them in the hierarchy; drawing from concepts associated with the Panopticon, she explains that a supervisor is the same thing as an overseer.[291] She emphasizes that throughout history, controlling and monitoring employees in the workplace is a central part of management; both recent technological developments and a management culture that emphasizes individual measurement and management have intensified individual monitoring.[292]

Despite the dangers, Ball is comfortable with the idea that surveillance at work is necessary and a normal element of working life that has been taken for granted.[293] She goes so far as to say that employees expect to have their performance reviewed and

---

[284] Kirstie Ball, "Workplace Surveillance: An Overview" (2010) 51:1 Labor History 87 at 87, online (pdf): *tandfonline* <www.tandfonline.com> DOI: <10.1080/00236561003654776> [Kirstie Ball, "An Overview"].
[285] *Ibid* at 88.
[286] *Ibid.*
[287] *Ibid.*
[288] *Ibid* at 89.
[289] *Ibid.*
[290] *Ibid.*
[291] *Ibid.*
[292] *Ibid.*
[293] *Ibid.*

information gathered on their activities and whereabouts—she says that this is a sign of good management practice.[294]

However, she finally admits that there are some controversies in this regard: when employee monitoring goes beyond what is considered reasonable or necessary; when employers demand exacting and precise information as to how employees use their time; and when the monitoring compromises working practices and negatively affects existing levels of control, autonomy, and trust.[295] Consequently, she explains that this is why some aspects of surveillance are considered acceptable to workers, while other aspects are opposed because they are considered to be too intrusive to workers.[296] She detects two concerns that go hand-in-hand: many employers lack specific policy provisions, and there is a lack of awareness of monitoring policies and practices among employees.[297]

For Ball, employers monitor performance and behaviours as part of ongoing production processes in real time, or personal characteristics as part of a one-off event to control access to the organization.[298] She provides some examples of the technologies involved for each type of monitoring. First, some examples of electronic measurements of performance include: keystrokes or telephone call content, or communications such as email and web monitoring.[299] Second, some examples of electronic tracking of behaviors include: location devices such as pagers, CCTV, GPS, and RFID, or covert surveillance (for instance, hidden cameras) to counter employee theft.[300] Third, some examples of electronic monitoring personal characteristics include: biometrics (bodily measurements such as electronic fingerprinting or retina and iris scanning), data mining, headhunting, and e-recruitment.[301] Ball notes that monitoring personal characteristics is more pervasive

---

[294] *Ibid.*
[295] *Ibid.*
[296] *Ibid.*
[297] *Ibid.*
[298] *Ibid* at 90–91.
[299] *Ibid.*
[300] *Ibid.*
[301] *Ibid.*

given that employers can make conclusions about employees' lifestyles, and this raises questions as to whether the employers should have this information.[302]

Ball casually notes that surveillance in the workplace is developing in respect of increased use of personal data, of biometrics, and covert surveillance; for instance, there is an increased use of human resources information systems or Internet activities such as e-recruitment and data mining of *curriculum vitae* databases.[303] She explains that "flipping" is becoming more common, whereby certain individuals covertly search for potential applicants by accessing user chat rooms or secretly going into organizations' Intranets to poach current employees.[304] But then she does recognize that there are privacy concerns associated with covert surveillance of email communications, especially since the employer has the capacity to record and store these communications.[305] She notes that this is because the communications may contain private conversations that include confidential information, and also information that could be stored on offshore servers in different jurisdictions that are subject to different rules.[306] Ball appreciates the fact that policies differ in workplaces, and this causes challenges for privacy protection.[307]

According to Ball, there are three main reasons why an employer would want to monitor employees: to maintain productivity and monitor resource use by employees; to protect corporate interests and trade secrets (this includes minimizing risks of defamation, sabotage, data theft, and hacking); and to protect the company from legal liability.[308] In fact, she points out that employee monitoring can serve as a significant risk management tool in order to limit costs and risks, protect value, and maintain quality.[309]

---

[302] *Ibid.*
[303] *Ibid.*
[304] *Ibid.*
[305] *Ibid* at 92.
[306] *Ibid.*
[307] *Ibid.*
[308] *Ibid.*
[309] *Ibid.*

Yet, Ball appreciates the dangers, namely, that excessive monitoring can be detrimental to employees when she states that privacy can be compromised if the employees do not authorize the disclosure of their information and it is subsequently broadcast to unknown third parties.[310] Also, she notes that there is the risk of function creep, as described by Andrejevic above.[311] And when employees know that they are being monitored, creative behaviour is reduced for fear of being judged negatively.[312] Further, Ball contends that using surveillance sends a strong message about what is expected and valued based on what tasks are monitored; monitored tasks are considered to be more valuable.[313] She points to another peril: there is a danger of "anticipatory conformity", where employees behave in docile and accepting ways, and this reduces commitment and motivation levels.[314] She admits that trust levels also reduce and can even be damaged when monitoring is improperly implemented.[315] Lastly, she cautions that excessive monitoring can actually produce the behaviours it was designed to prevent—when workers perceive excessive control using surveillance, they may manipulate the boundaries, sabotage the workplace, or simply refuse to comply with management's expectations.[316]

Ball elaborates on what can happen when employers use excessive electronic surveillance on employees; studies of call centers demonstrate that intense surveillance increases resistance, sabotage and non-compliance with management.[317] That is, workers who are extensively monitored are impacted quantitatively and qualitatively; they manipulate measures by dialing through call lists, leaving the lines open after the customer has already hung up, pretending to talk on the phone, providing minimal responses to customer queries, and misleading customers.[318] Likewise, the same can be said for managers who are under excessive electronic surveillance; they have been found to

---

[310] *Ibid* at 93–94.
[311] *Ibid* 90, 93–94; Mark Andrejevic, "Big Data Era", *supra* note 203
[312] Kirstie Ball, "An Overview", *supra* note 284 at 93–94.
[313] *Ibid.*
[314] *Ibid.*
[315] *Ibid.*
[316] *Ibid.*
[317] *Ibid* at 94.
[318] *Ibid.*

collude with workers in order to produce the desirable results.[319] Ball explains that workers apply "tacit knowledge", which means getting the better of monitoring, but not actively challenging the overall practice.[320] She notes that an example of more active employee resistance includes participating in "gripe" or "sucks" sites, where employees make online posts describing negative experiences they have with organizations.[321]

It is encouraging that Ball admits that privacy, ethics, and human rights issues are endemic to workplace surveillance.[322] Furthermore, she explains that discrimination in e-recruitment is also a major issue, especially since there is a temptation to create more of the same in an organization.[323] Indeed, the consequences of the panoptic sort manifest in the workplace, especially when relying on electronic surveillance technologies. Though she describes these considerations, she does not propose any solutions. But she explains that there are a few strategies to mitigate some of the negative consequences of employee monitoring by structuring task design, supervisory style, and employee cognition of monitoring.[324] For instance, she states that task design involves whether the employee has a choice in the pace and timing of their task; in situations where the monitoring is constant, it is likely that there will be more of an adverse effect compared to monitoring that is conducted intermittently or at regular intervals, and tasks that are not easily monitored must be evaluated in other ways.[325] Also, when supervisors rate employees negatively using monitoring, they are less likely to change their minds; also, workers tend to reach the same conclusions, and this leads to resistance and retaliation.[326] She proposes that the solution is to provide a mix of feedback and coaching that does not depend solely on monitoring, and when monitoring is used, supervisors need to clearly explain the criteria.[327] Also, cognitive factors relating to monitoring include employees' predispositions towards monitoring, and whether employees have a prior level of trust in

---

[319] *Ibid.*
[320] *Ibid.*
[321] *Ibid.*
[322] *Ibid* at 98.
[323] *Ibid* at 99.
[324] *Ibid* at 94–96.
[325] *Ibid* at 95.
[326] *Ibid.*
[327] *Ibid.*

the supervisors using monitoring; where employees perceive the monitoring as too invasive or unreasonable, the opposite of the desired effect can occur.[328]

What is most concerning is that, while Ball mentions that there are issues regarding how to balance competing interests in the workplace, she does not provide any solutions; for instance, she merely notes that there are issues when dealing with the question of allowing employees to blog publicly versus the employer's interest to covertly monitor off-duty Internet activity outside the workplace.[329] This is disappointing, because she presents an issue that amounts to the crux of the issue when it comes to electronic surveillance in employment, and leaves the reader hanging.

Therefore, although Ball provides information that is helpful for understanding the background concerning electronic surveillance in the workplace, and also some tips on how to monitor performance in the workplace using task design, supervisory style, and predispositions involving trust, she does not provide assistance on how to solve the more contentious problems that she describes. In particular, she points to some of the dangers that can lead to the abuse of surveillance power by employers, and their consequences, but she does not provide a balanced solution that allows for the respect of privacy of employees and the legitimate business needs of employers. She similarly does not spend sufficient time examining the trust dynamics in the employment relationship characterized by unequal bargaining power.

That said, Ball and Stephen T. Margulis together note that there are significant psychological effects associated with employee monitoring.[330] They caution that when employees experience stress due to monitoring, the consequences include physical symptoms such as pain (manifested as conditions such as repetitive strain injury and musculoskeletal discomfort), and psychological symptoms (manifested as conditions

---

[328] *Ibid.*
[329] *Ibid* at 98.
[330] Kirstie S Ball & Stephen T Margulis, "Electronic Monitoring and Surveillance in Call Centers: A Framework for Investigation" (2011) 26:2 New Technology, Work and Employment 113 at 116–117, online (pdf): *Wiley Online Library* <https://onlinelibrary.wiley.com/journal/1468005X> [Ball & Margulis, "Framework"].

such as low self-esteem, anxiety, and depression).[331] Further, Ball, Elizabeth M. Daniel, and Chris Stride recognize that employees are typically not permitted to make the same types of choices to protect their privacy compared to regular citizens and consumers, because they are usually subject to the working practices and environment dictated by their employers.[332] Additionally, they note that, in situations where employers provide effective data protection training dealing with the handling of customer data and privacy, employees' concerns about their own privacy increase; therefore, they recommend that employers also demonstrate that employee data is held in the same regard as customer data and worthy of similar treatment with strict rules and processes.[333]

To this point, I have discussed some important information regarding the nature of electronic surveillance in the workplace as explained by Ball and also Ball et al.

Now, I will move on and explore the effects of electronic surveillance on employees, considering the power imbalances at play.

For instance, Graham Sewell, James R. Barker, and Daniel Nyberg delve deeper into performance measurement and employee perceptions, and find that employees are likely to have one of two views when making sense of how and why surveillance is used to regulate conduct: "Care" and "Coercion" perspectives.[334] That is, the "Care" perspective views surveillance as a means of minimizing opportunistic behaviour such as free-riding, whereas the "Coercion" views surveillance as a means of increasing the subordination of an employee.[335] On one hand, the Care viewpoint entails using surveillance as a source of protection against antisocial behaviour and broadly legitimizes performance measurement in almost all circumstances since it is seen as beneficial.[336] On the other hand, the

---

[331] *Ibid* at 117.
[332] Kirstie Ball, Elizabeth M Daniel & Chris Stride, "Dimensions of Employee Privacy: An Empirical Study" (2012) 25:4 Information Technology & People 376 at 377, online (pdf): *Emerald Group Publishing* <www.emeraldinsight.com> DOI: <10.1108/09593841211278785> [Ball, Daniel & Stride, "Dimensions"].
[333] *Ibid* at 390.
[334] Graham Sewell, James R Barker & Daniel Nyberg, "Working under Intensive Surveillance: When Does 'Measuring Everything That Moves' Become Intolerable?" (2011) 65:2 Human Relations 189 at 190–191, online (pdf): *SAGE Journals* <hum.sagepub.com> DOI: <10.1177/0018726711428958>.
[335] *Ibid* at 191.
[336] *Ibid.*

Coercion viewpoint involves the phenomenon of the few watching the many in the interests of the few.[337] Sewell et al. state that, regardless of which viewpoint is taken, performance measurement is conducted in the same way—performance standards are set, performance is measured, and there is a determination of whether these standards are met when assessing individual performance.[338] They assert that this is a rational way of determining individual performance, and at this point, it is possible to draw on the results to assess outcomes such as setting remuneration levels, determining severity of punishment, and making disciplinary decisions—the answers to these questions depend which viewpoint is used.[339] For example, when using the Care viewpoint, performance measurement is considered to be protective since it serves the interests of the majority; it rewards employees who meet the norms of behaviour, and punishes employees who reject these norms.[340] In this scenario, the interests of the parties are mutual and the organizational dynamic is characterized by convergent interests because most recognize the legitimacy of the performance measurement.[341]

But it is clear that the Coercion viewpoint provides a more realistic picture of current workplace dynamics involving electronic surveillance. Sewell et al. find that, when using a Coercion viewpoint, the performance measurement is viewed as an instrument of domination seeking to subordinate the interests of the majority to those of the minority; consequently, this creates a situation where managers and employees have opposite interests, and where they pursue purposeful behaviors in order to further their interests.[342] Using this lens, the goal of performance measurement is for employers to maximize productivity and police the conduct of employees who must work at their maximum capacity.[343] They state that managers are the overseers who must ensure visibility of workers, and workers are the overseen who must avoid the managers' gaze.[344] In their efforts to maximize performance, the employers, the subjects of performance

---

[337] *Ibid.*
[338] *Ibid.*
[339] *Ibid.*
[340] *Ibid* at 195–197.
[341] *Ibid.*
[342] *Ibid* at 192–194.
[343] *Ibid.*
[344] *Ibid.*

management, identify the employees who fall above and below the acceptable standards, and provide rewards and punishments accordingly.[345] They contend that, an employer's goal is to eliminate autonomy, intensify work to unprecedented levels, and eliminate dissent.[346] In contrast, the employees, the members of the working class, become objects of performance measurement and wish to avoid subjugation and assert their autonomy.[347] They state that a broader dystopian vision of this dynamic would be intensive performance measurement that, if left uncorrected, would ultimately lead to the subjugation of employees as they recognize the futility of being disobedient.[348] Sewell et al. claim that this type of work dynamic can lead to various objections focusing on control and subordination; some examples include collective industrial action and manipulation or sabotage of performance management systems.[349] In fact, they contend that, when surveillance is everywhere, one consequence could be opposition at every opportunity through localized political activity.[350]

Sewell et al. study performance management in call centers and find that there are high levels of frustration as a result of the performance measurement involving close surveillance and constant comparison of performance levels among workers.[351] In fact, the workers view the performance measurement as an instrument of domination and express a sense of resignation about its impact.[352] It is unsettling that workers grudgingly express that there is little they can do to challenge this use of surveillance, to the point where it appears that there is an elimination of autonomy and a complete submission of the workers to the will of the managers and their performance management systems.[353]

Further, Sewell et al. also note that performance measurement can create or exacerbate asymmetrical power relationships in organizations as they can become forceful forms of

---

[345] *Ibid.*
[346] *Ibid.*
[347] *Ibid.*
[348] *Ibid.*
[349] *Ibid.*
[350] *Ibid.*
[351] *Ibid* at 202.
[352] *Ibid.*
[353] *Ibid.*

control or the focus of political struggles in the organization.[354] They suggest several questions that arise when scrutinizing the legitimacy of power relationships, including how much choice the workers have about the extent to which they are monitored.[355] Interestingly, when considering whether it is possible to prevent performance measurement from becoming oppressive, Sewell et al. note that at the individual level, it is common for surveillance to be viewed as onerous and offensive, while at the collective level, we often see surveillance as an essential means for maintaining important features such as fairness and social cohesion.[356] They state, "Like it or not, we are participants in our own understanding of organizational surveillance".[357] They question the political and ethical implications of ever-increasing monitoring in organizations, asking who gets to use it and for what purposes it is used.[358]

Pointing to the dangers of workplace electronic surveillance, Peter Jeffrey Holland, Brian Cooper, and Rob Hecker find that electronic monitoring and surveillance can have negative effects on the employment relationship through the loss of trust in management, particularly for manual workers.[359] What is discouraging is that this effect manifests as withdrawal behaviour, namely exiting the organization.[360] Holland, Cooper, and Hecker discuss trust in management as a critical element for organizations to foster in the workplace; they highlight that it is essential when seen as the basis for quality relationships, cooperation, and stability in the workplace.[361] Also, they emphasize the importance of trust in power relationships involving employers and employees.[362] Drawing on the social exchange theory, they see the employment relationship as a series of ongoing exchange relationships, which over time, establishes the nature and structure

---

[354] *Ibid* at 207.
[355] *Ibid* at 207.
[356] *Ibid* at 208.
[357] *Ibid.*
[358] *Ibid* at 208–209.
[359] Peter Jeffrey Holland, Brian Cooper & Rob Hecker, "Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type" (2014) 44:1 Personnel Review 161 at 161, online (pdf): *Emerald Insight* <www.emeraldinsight.com> DOI: <10.1108/PR-11-2013-0211>.
[360] *Ibid.*
[361] *Ibid* at 163.
[362] *Ibid.*

of the employment interactions; this is how reciprocity is manifested in the workplace.[363] They state that trust is the confidence that parties in the exchange have to not exploit each other's' vulnerabilities; the key characteristics of the trust relationship are ability, benevolence, and integrity.[364] By ability, they mean the expertise that facilitates the relationship, and by benevolence, they mean the intention to do good rather than simply seek rewards within the relationship.[365] They refer to integrity as the set of principles upon which the relationship is based that are acceptable and consistent, based upon previous interactions.[366]

Holland et al. warn that in situations of monitoring and surveillance, a balance must be struck between the parties to ensure the trust that underpins the employment relationship is not negatively affected.[367] They flatly reject the idea of, "if you are doing nothing wrong, you have nothing to fear";[368] rather, they insist that the relentless monitoring of employees can create a perception that the workforce cannot be trusted.[369] In fact, they argue that constant monitoring of work reflects distrust in the three main areas involving expertise, benevolence, and integrity.[370] Strategically speaking, they note that from a human resources (HR) perspective, high levels of trust are linked to employee commitment levels, overall organizational performance, employee well-being, and lower turnover rates.[371] And they clarify that HR management strategies involve using effective HR policies and practices that foster open communication, empowerment, and justice to increase trust in the employment relationship.[372]

Most disquieting, Holland et al. state that rapidly expanding electronic monitoring and surveillance techniques provide management with the opportunity to record work patterns, communications, and employee movements inside and outside the workplace,

---

[363] *Ibid.*
[364] *Ibid.*
[365] *Ibid.*
[366] *Ibid.*
[367] *Ibid* at 163–164.
[368] *Ibid* at 164.
[369] *Ibid.*
[370] *Ibid.*
[371] *Ibid.*
[372] *Ibid.*

while on-duty and off-duty; these capabilities increase the perceived level of control over the workforce and affect the balance of trust in the employment relationship.[373] They highlight that these technologies can create significant tensions and stressors in the employment relationship and actually contribute to the erosion of employment relations through the increased powerlessness of the employee.[374] Accordingly, they contend that controlling electronic surveillance technologies aimed at forced obedience can send a contradictory message to employees and negate the impact of effective HR policies and practices that are based on trust.[375]

Ultimately, Holland et al. confirm with their study that electronic monitoring and surveillance is connected to overall trust in management—employees who report their employers as being deceptive increase with the number of electronic monitoring and surveillance practices used in the workplace.[376] These employees also report that they have a lower perception that management can be trusted to make sensible or competent decisions for their organization when there are more monitoring and surveillance technologies present in the workplace.[377] It appears that increased use of electronic monitoring and surveillance practices can induce a negative perception of management and affects the employment relationship in a way that undermines trust.[378] These effects are significantly more present with manual workers who are subject to more overt and continuous electronic surveillance practices such as overt cameras and electronic tracking.[379] Thus, Holland et al. recommend that employers develop a balanced policy strategy that promotes the fostering of trust in the employment relationship in regards to electronic monitoring and surveillance techniques in the workplace.[380]

---

[373] *Ibid* at 164–165.
[374] *Ibid* at 165.
[375] *Ibid.*
[376] *Ibid* at 169.
[377] *Ibid.*
[378] *Ibid.*
[379] *Ibid* at 169 –171.
[380] *Ibid* at 171.

But it is Zuboff who most thoroughly examines electronic surveillance and power dynamics in the workplace—and effectively stresses the concerns.[381] She states that when authority fails, managers frequently look to a second dimension of power, which she calls a "technique".[382] She claims that these techniques are essentially management practices that shape and control behaviour.[383] She contends that techniques such as surveillance constitute a source of comfort and relief for authority figures because they circumvent the imperfections of imperative control.[384] Zuboff boldly states that the techniques of control effectively diminish the likelihood of disobedience because there is a probability of detection.[385]

Zuboff draws on the Panopticon to show that the techniques of control in the workplace, through the use of computers at work, have a considerable impact on the American pulp mills she studies; that is, the "Overview System" present in one of the companies she examines enables visibility throughout the plant and allows management to observe and discipline employees based on the system's output.[386] More explicitly, she states:

> Information systems that translate, record, and display human behaviour can provide the computer age version of the universal transparency with a degree of illumination that would have exceeded even Bentham's most outlandish fantasies. Such systems can become information panopticons that, freed from the constraints of space and time, do not depend upon the physical arrangement of buildings or the laborious record keeping of industrial administration. They do not require the mutual presence of objects of observation. They do not even require the presence of an observer. Information systems can automatically and continuously record almost anything their designers want to capture, regardless of the specific intentions brought to the design process or the motives that guide data interpretation and utilization. The counterpart of the central tower is a video screen.[387]

---

[381] Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York: Basic Books, 1988) [Shoshana Zuboff, "Smart Machine"].
[382] *Ibid* at 313.
[383] *Ibid.*
[384] *Ibid.*
[385] *Ibid.*
[386] *Ibid* at 315−361. The Overview System is a plant-wide control system that receives real-time data to obtain a snapshot of what is happening in the plant. This surveillance system is used at the Cedar Bluff plant. See the methodology section in Appendix B at 423–429, and also the initial discussion about the system at 324–327.
[387] Shoshana Zuboff, "Smart Machine", *supra* note 381 at 322.

Zuboff explains why managers would want to use panoptic power, referring to the constant pressures that are on managers to provide feedback, listen, coach, manage objectives, provide vision, and so on.[388] What is more, the authority relationship is one of mutual dependency, characterized by reciprocity, where the manager and the managed have the means to counter the behaviour of the other.[389] Given that this relationship of reciprocity requires significant psychological effort to maintain, she states that it is tempting for managers to avoid reciprocal relationships and instead rely on the alternative technique of control and panoptic power.[390] She points to the alarming fact that the technique of surveillance enables management to refrain from dealing with face-to-face interactions altogether simply by using the presence of the omniscient observer.[391]

Zuboff notes the relevant business interests, and finds that the Overview System enables management to observe a wide range of behaviours for: evidence of irregularities for coaching and disciplining; opportunities to accelerate learning and improve performance; avoidance of personal supervision to allow managers to distance themselves from subordinates; and a transformation of administrative assumptions and practices of the managerial hierarchy.[392] Still, she discovers that, at each level of the organization she studies, workers constantly search for ways to adapt to the intense illumination of the information Panopticon—she states that the workers recognize the Overview System's supervisory power and try to accept the nature of the involuntary display.[393] In one interview, one worker claims that the system can be used to see how workers are doing, and that is a good thing, unless someone is trying to hide something; the worker notes that is not possible to hide mistakes from the system.[394] Zuboff states:

> To some, it seemed that only the human heart retained its privacy, out of reach and recalcitrant.[395]

---

[388] *Ibid* at 323.
[389] *Ibid.*
[390] *Ibid.*
[391] *Ibid.*
[392] *Ibid* at 324–327.
[393] *Ibid* at 342
[394] *Ibid.*
[395] *Ibid.*

Zuboff explains that a lack of confidence in the shared values of the authority relations can ultimately lead to a situation where superiors doubt their own legitimacy and turn to a technique as a means of enforcement; in turn, subordinates "cast about for extralegitimate techniques of defence".[396] This leads to the use of adversarial vocabulary, including "us" versus "them", and as a result, mistrust is "invoked in the silent dance of the observer and the observed".[397] Zuboff cautions that visibility creates a sense of vulnerability and powerlessness, and causes the observed to question whether they are being exposed in ways they would not wish to be exposed.[398] Consequently, the observed resists such exposure in order to retain a sense of self-control either by circumventing the observer to reduce power in the Panopticon, or by anticipating behavioural expectations of the observer to conform to standards (anticipatory conformity).[399] Zuboff insists that many workers cherish autonomy and a sense of self-control, and when they contemplate the prospect of a socially integrated high-technology workplace, they feel despair.[400] In particular, they anticipate a loss of their unique identities and freedom, and fear that without traditional sources of protection set out in their job descriptions and employment contracts, they will "become prey to every capricious whim of management".[401]

To recap, I have just explained the theories that deal with electronic surveillance inside the workplace. This side of the coin was important to examine, since these ideas directly apply in the employment context. As can be seen above, there are some notable challenges when it comes to electronic surveillance in the workplace, given the power imbalances, as explained by theorists such as Sewell et al., Holland et al., and Zuboff.

I will now do the last thing that I said I would do—I will pave the way to Chapter 3 by explaining why the surveillance theorists' views of privacy are problematic, and argue that it is necessary to have individual privacy protections as conceptualized by the privacy theorists that are discussed in Chapter 3.

---

[396] *Ibid* at 344.
[397] *Ibid.*
[398] *Ibid.*
[399] *Ibid* at 344–345.
[400] *Ibid* at 404.
[401] *Ibid.*

2.4 The Problem with Surveillance Theorists' Views of Privacy

In this part, I will highlight the challenges associated with surveillance theorists' views of privacy and argue that it is necessary to create individual privacy protections as conceptualized by privacy theorists.

Let me begin with Monahan and Wood. They state that privacy is the thing that most people think of as being compromised by surveillance.[402] As they put it:

> It may seem counterintuitive, especially given the centrality of privacy in public discourses about surveillance, but the field of surveillance studies has an uncomfortable relationship with the privacy concept, sometimes bordering on an aversion.[403]

Why is there such an aversion? Monahan and Wood draw on several critiques and suggest that this phenomenon could be because of the argument that an individual concept of privacy is poorly suited to account for discrimination against groups, does not fully consider marginalized populations with issues of domination and survival, and it is universalizing to the point that it is unable to address issues of power imbalances.[404]

In line with Monahan and Wood's comments, Priscilla Regan emphasizes that there is an overreliance on an individualistic framing of privacy whereby privacy is considered important to the individual and is viewed as some type of boundary that shields the individual from others.[405] She contends that this is because the idea of privacy is rooted in liberal thinking, where privacy is considered to be an essential part of the individual for self-development and human relationships.[406] Regan asserts that, as a result, policy discussions focus on protecting an individual value or interest in privacy.[407] Regan states that privacy has a framing problem that views privacy primarily as a value to the

---

[402] Monahan & Wood, "Privacy and Autonomy" in Monahan & Wood, *supra* note 101, 209 at 209 [Monahan & Wood, "Privacy and Autonomy"].
[403] *Ibid* at 210.
[404] *Ibid.*
[405] Priscilla M Regan, *Legislating Privacy* (North Carolina: The University of North Carolina Press, 1995) at 24.
[406] *Ibid.*
[407] *Ibid.*

individual, and as such, "this line of discourse has served to weaken the concept of privacy as a policy goal".[408] She states that this inaccurate framing creates the lack of development of a broader social importance to privacy.[409] More precisely, she states, "When privacy competes with another social value or interest, the *social* basis of the other interest is explored while the *individual* basis of the privacy interest is examined".[410] Also, Regan asserts that privacy is not absolute and has to be balanced against other rights and interests—and it usually loses the competition.[411] She explains that in policy debates, the individual interest is on a weaker footing than a societal interest; privacy is on the defensive because it has the burden of proving that certain activity invades privacy and that the individual privacy interest is more important than the societal interest.[412]

Therefore, Regan states that privacy is a common value (all individuals value some privacy), public value (it involves the democratic political system as well as the individual), and collective value (all persons have the same minimum amount of privacy).[413] Thus, it is important to explicitly acknowledge the social importance of privacy.[414] Regan insists that rather than individual preferences, privacy's importance can come from a sense of connection and mutuality; recognizing these common foundations could change the nature of policy debate and create stronger public policy privacy protection.[415]

Likewise, Jean-François Blanchette and Deborah Johnson argue that it is important to view privacy in terms of the social benefits of forgetfulness, rather than in terms of individual privacy protection.[416] They conclude that data retention and disposal should be

---

[408] *Ibid.*
[409] *Ibid* at 24, 33.
[410] *Ibid* at 27.
[411] *Ibid.*
[412] *Ibid* at 22–23.
[413] *Ibid.*
[414] *Ibid* at 214.
[415] *Ibid.*
[416] Jean-François Blanchette & Deborah G Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness" (2002) 18:1 The Information Society 33 at 33−34, online (pdf): *Taylor & Francis* <www.tandfonline.com> DOI: <10.1080/01972240252818216>.

addressed as a part of a broader and comprehensive policy approach rather than in a piecemeal fashion or *ad hoc*.[417] Blanchette and Johnson state that in the past, there has been an institutional forgetfulness that parallels the human memory—the paper-and ink world has several challenges of archiving, storage space, and budgeting for file cabinets.[418] The electronic environment favours data retention, and this has changed in the default position from forgetfulness to one of memory.[419] They say that currently, we are in a world that captures endless data and decides how long to retain it; they question the social implications of the lack of institutional forgetfulness.[420]

Further, they assert that privacy is both an individual good and a social good, and these goods are inextricably tied together.[421] They state that privacy is good for society because it promotes the development of individuals in a way that is good for democracy.[422] They argue that, where there is no forgetfulness because everything is recorded and never forgotten, it creates a world that is not conducive to the development of democratic citizens.[423] Thus, it is important to achieve a balance between the appropriate degree of social forgetfulness and the need to hold people accountable.[424] They examine the areas of bankruptcy law, juvenile crime records, and credit reporting and note that, in these areas, there has been a historical recognition of the social value of forgetfulness.[425] However, social forgetfulness is an important social value that is quietly slipping away.[426] As a result, they claim that, instead of balancing social goods of information against individual rights or interests of privacy, there should be an understanding that involves "tensions between social goods, the social good of privacy (and forgetfulness), and other social goods".[427] They state that data retention must be addressed as part of a comprehensive data protection policy that consistently uses a variety of strategies

---

[417] *Ibid* at 43.
[418] *Ibid* at 34.
[419] *Ibid.*
[420] *Ibid* at 34–35.
[421] *Ibid* at 36.
[422] *Ibid.*
[423] *Ibid.*
[424] *Ibid.*
[425] *Ibid* at 36–38.
[426] *Ibid* at 39.
[427] *Ibid.*

including an overarching set of standards, legislation in specific sectors, a structured market, and privacy-enhancing technologies.[428]

Along the same lines, Julie E. Cohen states that privacy has an image problem, since it is "cast as old-fashioned at best and downright harmful at worst".[429] Indeed, she views it as "anti-progressive, overly costly, and inimical to the welfare of the body politic".[430] Cohen asserts that the consequences of privacy's bad reputation is predictable; when balancing outdated values against cutting edge imperatives like national security, efficiency, and entrepreneurship, "privacy comes up the loser".[431] She suggests that, since privacy has been conceptualized as a form of protection for the liberal self, it is reactive and inessential, and could chill the exercise of constitutionally protected liberties.[432] Cohen clarifies that this type of thinking is mistaken, and the liberal self who is the subject of privacy theory and privacy policy making does not actually exist.[433] Indeed, she states that the self who is the real subject of privacy law and policy is socially constructed.[434] Cohen insists that viewing privacy as an individual right is a mistake.[435]

Cohen states that privacy's inadequate conceptual vocabulary, along with its inadequate institutional grammar, leads to significant contradictions in terms of privacy theories.[436] However, she believes that these contradictions can constitute an opportunity to "turn privacy inside out".[437] Cohen wants to rescue privacy theory by focusing on the conditions that are needed to produce sufficiently private and privacy-valuing subjects (for individuals), and by focusing on the design, production, and operational practices best suited to preserve those conditions (for institutions).[438] Cohen states that it is

---

[428] *Ibid* at 39–43.
[429] Julie E Cohen, "What Privacy is For" (2013), 126:7 Harvard Law Review 1904 at 1904 [Julie E Cohen, "Privacy is For"].
[430] *Ibid.*
[431] *Ibid.*
[432] *Ibid.*
[433] *Ibid.*
[434] *Ibid.*
[435] *Ibid* at 1927.
[436] Julie E Cohen, "Turning Privacy Inside Out" (2019) 20.1:1 Theor Inq L at 1, online (pdf): *ProQuest* <https://search-proquest-com> DOI: <10.1515/til-2019-0002> [Julie Cohen, "Inside Out"].
[437] *Ibid* at 2.
[438] *Ibid* at 3.

problematic to justify privacy in a way that promotes and protects individual autonomy, because the experience of having identities and making choices is socially shaped.[439] Similarly, she finds it problematic to justify privacy in terms of dignity because she says that this creates similar paradox—like experienced subjectivity, conceptions of dignity are culturally constructed.[440] In particular, different societies articulate dignity differently and have different norms.[441] Cohen does not agree that privacy is justified because it promotes and protects an essential degree of separation between the self and society for dissent and critique.[442] She goes so far as to say that formulations of privacy in the liberty-based language of human rights discourse are grand, inspiring, and difficult to dispute—but they are also "operationally meaningless".[443]

Lastly, Colin Bennett discusses several objections to privacy theorists' views of privacy, and defends the concept of privacy using the surveillance theorists' conceptions instead.[444] Bennett points out that there are several framing problems associated with the concept of privacy as described by privacy theorists.[445]

First, Bennett maintains that there tends to be a reinforcement of individuation, rather than community, sociability, and trust—he describes it as, "It is about me, and nobody else".[446] He asserts that individualistic conceptions of privacy do not capture the whole problem because privacy is not the sole answer.[447] Second, Bennett states that there are spatial implications inherent in privacy discourse whereby there is a type of bubble that surrounds each person in a cell that others cannot invade.[448] He insists that, practically speaking, it is not possible to protect the bubble because the issue is more complex and

---

[439] *Ibid.*
[440] *Ibid* at 4.
[441] *Ibid.*
[442] *Ibid.*
[443] *Ibid* at 6.
[444] Collin J Bennett, "In Defence of Privacy: The Concept and the Regime" (2011) 8:4 Surveillance & Society 485, online (pdf): *Surveillance & Society* <http://www.surveillance-and-society.org> [Colin Bennett, "In Defence of Privacy"].
[445] *Ibid* at 485–486.
[446] *Ibid* at 486–488.
[447] *Ibid.*
[448] *Ibid* at 488–489.

relational.[449] Third, Bennett contends that it is problematic when privacy is articulated as a "right" because privacy battles tend to pit vulnerable individuals, or poorly resourced civil liberties groups, against very powerful public or private organizations.[450] He posits that there is an emphasis placed on controlling excessive surveillance rather than the private interest in privacy protection, individual privacy claims are limiting in that they do not necessarily trigger regulatory action, and rights discourse fails to serve the people most at risk since they cannot fit their experiences of surveillance into a legal claim.[451] Fourth, Bennett explains that the concept of privacy and policies never challenge larger questions of categorical discrimination; to him, the problem *is* discrimination, not privacy, since individuals are at risk merely because of their membership in a group, rather than because of their individual identities and personal information they generate.[452] Fifth, Bennett contends that the concept of privacy is too narrow; even though it is conceptually confusing and vague, "still leaves aside a number of crucial questions that surveillance scholars take very seriously".[453] For example, there is a problem with determining the point at which information becomes personal information (as seen with re-identification of data); also, power relations are present between the watcher and watched even when personal information is not collected (as can be seen when the presence of cameras changes behaviour, even if they are not monitored or operational).[454] He states, "It is in these examples that we find, I think, the crucial point at which privacy analysis ends and surveillance analysis begins".[455]

However, Bennett's assertions regarding surveillance theorists' views of privacy can be rebutted. Firstly, it remains a fact that privacy regimes are necessary in order to affect meaningful change and protect citizens from the abuse of surveillance power. What also weakens the individualistic argument is that groups of individuals can benefit from making privacy claims and privacy disputes do not necessarily involve only one

---

[449] *Ibid.*
[450] *Ibid* at 489–490.
[451] *Ibid.*
[452] *Ibid* at 490–491.
[453] *Ibid.*
[454] *Ibid.*
[455] *Ibid.*

individual in a “me, me, me” situation; for instance, there could be groups of people in a privacy dispute such as a group of employees, and this redistributing of power can benefit society as a whole and create a social good. Secondly, it is a natural human need for individuals to want to exercise self-determination and autonomy by setting healthy spatial boundaries. Thirdly, it is problematic to discount the balancing of interests for four reasons. Here is the first reason: when balancing interests, it is not a necessary condition for both parties to have exactly the same level of power in a privacy dispute; in fact, in most surveillance scenarios, one party is more vulnerable than the other, and this does not make the balancing of interests any less important. Here is the second reason: the reason for attempting to control excessive surveillance is because there needs to be a limit to establish when one has crossed the line and gone too far to ensure the dominant party is not abusing its surveillance power. Here is the third reason: it is not necessary for regulatory action to be triggered every time there is a privacy dispute; over time, decision makers become attuned to what is happening on a grand scale so that decisions can evolve with societal values. Here is the fourth reason: it is indeed possible to make and succeed with legal claims.

Fourthly, against the suggestion that discrimination is the real problem, it is more likely that discrimination is rather a consequence of the abuse of surveillance power that leads to the excessive surveillance of the weaker party and the privacy intrusion, which causes additional information to be learned. Without the abuse of surveillance power and consequent privacy intrusion in the first place, the information would not be discovered, the panoptic sorting would not take place, and discrimination would not take place. Fifthly, the contention that privacy is too narrow is likely exaggerated. One may question whether there is a crucial point at which privacy analysis ends and surveillance analysis begins. Another way of looking at this issue is that surveillance theorists and privacy theorists both take crucial questions seriously; they just approach the issues from different angles.

Ultimately, Bennett insists that the critiques of surveillance theorists address a dated conception of privacy with a framing that only partially covers privacy protection in practice and that ineffectively addresses power imbalances between individuals and

organizations that use the latest information technologies.[456] Yet, Bennett finally admits that realistically speaking, without privacy regimes, there would be few if any actual mechanisms of social redress.[457] He states that privacy as a concept and regime is resilient and will not disappear, and surveillance scholars must live with it.[458]

To this point, I have explained the views of surveillance theorists such as Regan, Blanchette and Johnson, J. Cohen, and Bennett when discussing conceptualizations of privacy I have also rebutted the main arguments of the theories in order to show why it is important to examine the privacy theories set out in Chapter 3.

Now, I will look at one more thing—I will delve into ideas regarding resistance and opposition, which involve actions that are taken in response to surveillance and that are in line with one's views of privacy.

That is, while surveillance theorists may disagree with the framing of privacy and have an uncomfortable relationship with the privacy concept, it is important to recognize their ideas involving opposition and resistance. Lyon notes that in each case, objections are raised and expressed to some surveillance process where individuals feel that some line has been crossed.[459] Monahan and Wood explain that when it comes to surveillance, some have strong reactions and work to challenge the abuses of power.[460] On one hand, resistance involves quieter practices that seek to avoid or otherwise manage a system; one example is when people install ad-blocker programs on their web browsers.[461] On the other hand, opposition involves public efforts to block or significantly change policy; an example involves public campaigns and lawsuits by groups such as the American Civil Liberties Union (ACLU) or the Electronic Frontier Foundation (EFF).[462]

---

[456] *Ibid.*
[457] *Ibid.*
[458] *Ibid.*
[459] David Lyon, "Surveillance Studies", *supra* note 109 at 166.
[460] Monahan & Wood, "Resistance and Opposition" in Monahan & Wood, *supra* note 101, 331 at 331 [Monahan & Wood, "Resistance and Opposition"].
[461] *Ibid.*
[462] *Ibid.*

More specifically, with respect to resistance, Gary T. Marx explains that most surveillance systems have inherent contradictions, ambiguities, gaps, blind spots and limitations; the natural human tendency is to attempt to beat surveillance systems and avoid observation.[463] He proposes 11 techniques that are focused on resisting particular privacy-evading information technologies.[464] They include: discovery moves (also called surveillance detection in the intelligence trade, where the goal is to find out if surveillance is in operation and where it is); avoidance moves (passive withdrawal); piggybacking moves (control is evaded or information is protected by attaching it to a legitimate subject); switching moves (in testing situations, authentic results are transferred to someone else); distorting moves (manipulating the surveillance collection process so that invalid inferences are drawn); blocking moves (calling explicit attention to the communicative aspects of surveillance where subjects physically block access to the communication to render the information unusable); masking moves (manipulation beyond blocking, in order to deceive regarding identity, status, and so on); breaking moves (rendering the device inoperable in the crudest form); refusal moves (moving away from participation or just saying "no"); cooperative moves (insider perpetration in cooperation with violators beyond the organization); and counter-surveillance moves (turning around and conducting surveillance on the watchers).[465]

An example of resistance is counter-surveillance move that Steve Mann, Jason Nolan, and Barry Wellman call "sousveillance", coming from the French words for "*sous*", meaning "below" and "*veiller*", meaning "to watch".[466] They state that individuals use tools to observe the organizational observer in order to enhance the ability to assess and collect data about their surveillance and to neutralize it.[467] They contend that digital

---

[463] Gary T Marx, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance" (2003) 59:2 Journal of Social Issues 369 at 369–370, online (pdf): *The Society for the Psychological Study of Social Issues* <https://spssi-onlinelibrary-wiley-com> DOI: <10.1111/1540-4560.00069>.
[464] *Ibid* at 372, 388.
[465] *Ibid* at 374–384.
[466] Steve Mann, Jason Nolan & Barry Wellman, "Sousveillance: Inventing and Using Wearable computing Devices for Data Collection in Surveillance Environments" in Monahan & Wood, *supra* note 101, 347 at 347.
[467] *Ibid* at 348.

technology can help individuals feel more empowered.[468] They note that sousveillance disrupts the power relationship of surveillance and restores balance.[469] Jean-Gabriel Ganascia states that sousveillance is made possible because we are living in the Catopticon, where there is total transparency, and this allows everyone to watch, communicate, and consequently control each other.[470]

Another example of resistance is a masking technique whereby artistic projects are generated to conceal oneself from ambient surveillance in public places; Manahan states that the goal is to mask identity to undermine technological efforts to separate someone from the crowd.[471] These strategies can involve such things as face paints, hairstyles, hoodies, scarves, materials that block thermal emissions to avoid tracking by drones, and hats that emit infrared light to blind camera lenses.[472] Manahan explains that, in this way, individuals may hide in plain sight without having to acquiesce to the surveillance or end up becoming a recluse to avoid the gaze.[473]

One more example of resistance is a distorting move that Finn Brunton and Helen Nissenbaum call, "obfuscation".[474] They explain that obfuscation is the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection.[475] It can be understood as the production of noise in order to make data collection more ambiguous, confusing, harder to exploit, difficult to act upon, and therefore less valuable.[476] For example, one strategy that can be used to

---

[468] *Ibid.*
[469] *Ibid* at 350.
[470] Jean-Gabriel Ganascia, "The Generalized Sousveillance Society" (2010) 49:3 Social Science Information 449 at 497, online (pdf): *SAGE Publishing* <www.sagepub.co.uk> DOI: <10.1177/0539018410371027>.
[471] Torin Monahan, "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance" (2015) 12:2 Communication and Critical/Cultural Studies 159 at 159, online: *Taylor & Francis* <www.tandfonline.com> DOI: <10.1080/14791420.2015.1006646> [Torin Monahan, "The Right to Hide?].
[472] *Ibid* at 159–160.
[473] *Ibid* at 160.
[474] Finn Brunton & Helen Nissenbaum, *Obfuscation: A Users Guide for Privacy and Protest* (Cambridge, MIT Press, 2015).
[475] *Ibid* at 1.
[476] *Ibid* at 46.

interfere with surveillance and data collection is a software strategy that prevents profiling of user searches by blending genuine and artificial search queries.[477]

With respect to opposition, Colin Bennett thoroughly examines opposition actors, "privacy advocates", who he defines as "people who, at least in journalistic parlance, challenge the development of the increasingly intrusive ways by which personal information is captured and processed".[478] He notes that there are several groups that promote the cause of personal privacy protection; the types of groups include privacy-centric advocacy groups (such as Privacy International), privacy advocacy and civil liberties (such as the ACLU), privacy advocacy and human rights (such as Amnesty International), privacy advocacy and consumer protection (such as the Privacy Advisory Group), and privacy advocacy and digital rights (such as the EFF).[479] He contends that there are several privacy advocacy types, including activists, researchers and teachers, consultants, technologists, journalists, and artists.[480] He states that, while these individuals make up an extremely diverse group, they have one thing in common—they are animated by a fundamental belief that privacy is critical.[481]

I have just explained the surveillance theorists' views of privacy. I noted that these conceptualizations are problematic, and that there is a need to explore the privacy theories in Chapter 3. I also explored some of the resistance and opposition strategies individuals use in response to surveillance that are in line with their views of privacy.

2.5 Conclusion

As explained in the opening of this Chapter, the study of surveillance is a transdisciplinary field made up of a large number of different perspectives and theories. Taken together, the surveillance theories paint a fuller picture of the nature of electronic surveillance that can be encountered both inside and outside the workplace. In each

---

[477] *Ibid* at 13.
[478] Colin J Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008) at ix [Colin Bennett, "Privacy Advocates"].
[479] *Ibid* at 28–49.
[480] *Ibid* at 60–94.
[481] *Ibid* at 94.

category, there are a handful of theorists that do not necessarily disagree; in fact, the theories discussed simply build on each other and enhance knowledge from various vantage points when describing the nature and implications of surveillance. It was important to investigate these instructive surveillance theories explaining the complicated nature of electronic surveillance technology because I will be relying on the information in my analyses in Chapters 4 and 5; these analyses will provide the necessary foundation for creating the new workplace privacy regime.

If we picture a coin as the employment context, then ubiquitous surveillance and workplace surveillance are two sides of that same coin: ubiquitous surveillance theories are involved indirectly (outside the workplace), and workplace surveillance theories are involved directly (inside the workplace). If we imagine the rim of that coin running through and affecting both sides of that coin as the Panopticon, we can view it as a vital component that touches on both ubiquitous and workplace surveillance theories. And if we step back and use a particular lens when examining this coin, that lens is the capitalist surveillance perspective of surveillance.

I examined selected categories of surveillance theories, beginning with the Panopticon. This was the starting point for the study of surveillance. I noted that the design goal of the Panopticon was to reverse the logic of the dungeon by spreading light and reason to the dark space where evil might flourish using illumination; the architecture of the building played a crucial role in understanding how the combination of daylight, interiorization, and the overseer's gaze increased visibility. These panoptic concepts work to dominate and control individuals both inside and outside the workplace.

I also investigated several theories involving ubiquitous surveillance. These theories highlight what can happen when electronic surveillance is conducted in the outside world, and the information is subsequently obtained and used in the workplace to make employment decisions regarding employees. The theories surveyed several topics associated with ubiquitous surveillance, including the nature of electronic surveillance and the temporal dimensions involved (timeframe, intensity, persistence of consequences, and time period). In addition, the theories discussed sophisticated automated data

processing and big data surveillance; not only has the level of sophistication increased, but so too has the opportunity for conducting electronic surveillance because surveillance is everywhere and can be used by governments, employers, and businesses. That is, we live in a surveillance society. The theories also cover core issues dealing with social media and how, though it can be fun, we ultimately participate in our own surveillance when we use these platforms and create user-generated content. As a consequence, we open ourselves up to exploitation.

I then considered theories concerning surveillance inside the workplace. The workplace surveillance theories provided insights on how common it is to monitor employees in the workplace, the technology types involved in the electronic surveillance of employees, the concerns about excessive and overly intrusive surveillance, and the effects of electronic surveillance on employees when an employer's surveillance goes too far. The theories also considered the impact of electronic surveillance on trust in the employment relationship, and the detrimental effects of excessive monitoring on employees. The workplace surveillance theories also explored why employers monitor employees, and how employees cannot make the same kinds of surveillance decisions as regular consumers because they are subject to the direction of their employers. Workplace surveillance theories also explained the Coercion viewpoint of electronic surveillance; the aggravating effect of electronic surveillance on asymmetrical power relationships; the need to strike a balance between the parties when dealing with electronic surveillance in an employment relationship; and the power dynamics involved with electronic surveillance in the employment relationship.

Finally, I noted the problems with surveillance theorists' take on privacy. I explained that surveillance theorists have an uncomfortable relationship with the idea of privacy, mostly because they believe that there are problems with the framing of the concept. For example, they do not like that privacy is individualistic, competes with other rights that are valued by society, and can be considered a human right. I set out several challenges with the way that surveillance theorists view privacy. Indeed, there is an eventual admission that traditional conceptions of privacy are the main way to obtain redress from excessive surveillance; I also reviewed some types of opposition and resistance strategies

regarding how individuals respond to surveillance. I noted that it was necessary to examine privacy from the considerably distinct and disparate theories of privacy in Chapter 3. This section served as a transition from Chapter 2 to Chapter 3.

I examined the surveillance theories using a capitalist surveillance perspective of surveillance, which emphasizes the dangers of electronic surveillance and opposes the exploitation of individuals in the surveillance economy. It is clear that surveillance is about control—it all starts with the Panopticon. The increased visibility, internalization, and constant gaze create a transparency which Foucault views as a trap, since the watched ultimately self-censor and modify their own behaviour in order to become obedient. The invisible watchers exert their power by ensuring compulsory visibility of the watched, and this causes a situation where the watched are constantly worried about being monitored by anonymous invisible observers.

The Panopticon is a foreshadowing of what presently occurs in general society and in the workplace. Foucault's profoundly disturbing image of a circular cage does not stop with the Panopticon. Rather, the effect continues firstly with ubiquitous surveillance in modern times. Social media use is a good example of how information is collected and aggregated to compile a profile of each individual that can be used by private corporations when making decisions, including employment decisions. The watcher no longer begins the process with picking a suspect to monitor due to suspicion—the watcher simply watches everyone continuously and generates subjects. Since the goal of private corporations involves making future predictions, data becomes a form of power when it is used to manipulate people and shape the information they see. Modifying human behaviour is accomplished by discovering behavioural surplus, the extra data exhaust left over after engaging in various online services, and this surplus is used to make predictions about user behaviour and ultimately control the behaviour through the use of learning theories and the sale of information to companies in the behavioural futures markets. Clearly there is a concern, especially since this phenomenon has a potential of leading to the inevitable situation where we as humans have no ability to control anything about our lives—we could be left without a sense of self-determination.

In this scenario, the watched are simply pawns in a game, and there is the dangerous possibility of discrimination based on what information emerges from the panoptic sort.

This is not all. The effect continues secondly with even more noteworthy opportunities for employers to abuse their surveillance power against the weaker employees specifically in the workplace. Essentially, surveillance functions as a way of controlling employees. The employers, the overseers in this panoptic arrangement, have a high potential to abuse their surveillance power without the proper checks in place. While many accept that monitoring in the workplace is nothing new and a sign of good management practice, there is reason for concern. There are times when the monitoring can go too far and go beyond what is reasonable, and the undesired intrusiveness affects trust in the employment relationship. This is so, whether the employer is monitoring employees' performance, behaviours, or personal characteristics. This applies regardless of whether the goal of monitoring is used for maintaining productivity and efficiency, protecting corporate interests and trade secrets, or protecting the company from legal liability. The problem is that workplace monitoring can be detrimental to employees when it goes too far or is too intrusive, when there is function creep involved, when employees experience anticipatory conformity, when employees become docile and accepting to the point where their commitment and motivation levels are reduced, and when trust levels are reduced. As a result, employees may feel that they have no choice but to manipulate work rules, sabotage the workplace, or refuse to comply with management. Other negative consequences involve troubling effects of discrimination due to the panoptic sort, and physical and psychological symptoms.

Since employees do not have as many choices about the extent of surveillance to which they are subjected compared to regular consumers and citizens, they are more vulnerable. The Coercion model clarifies that employment involves the few watching the many in the interests of the few. The goal of performance management is for employers to maximize productivity and police the conduct of employees who must work at their maximum capacity. Managers are the overseers who must ensure visibility of workers, and the workers are the watched who must avoid the managers' gaze. Indeed, the employees become the objects of performance measurement, try to avoid subjugation, and attempt to

assert their autonomy. Without anything in place to protect the employees, the result is the ultimate subjugation of employees, where resistance would be futile. Indeed, employees view performance measurement as an instrument of domination and feel that there is nothing that can be done about the surveillance. This causes an exacerbation of the unequal bargaining power in the employment relationship, and leaves employees wondering if they have any choice at all regarding the extent of the employer's monitoring. What is most troubling is the effect of trust in the employment relationship in cases of an employer's use of electronic surveillance. When there is monitoring in the workplace, the result is distrust in the areas of expertise, benevolence, and integrity. A useful approach to dealing with electronic surveillance in the workplace is to create a balanced strategy that respects trust in the relationship.

Chapter 3

3 Social Theory: Examination of Privacy Theories

> The point is not the hypocrisy of those who disparage the value of privacy while intensely safeguarding their own, although that is striking. It is that the desire for privacy is shared by us all as an essential, not ancillary, part of what it means to be human. We all instinctively understand that the private realm is where we can act, think, speak, write, experiment, and choose how to be, away from the judgmental eyes of others. Privacy is a core condition of being a free person.
>
> —Glenn Greenwald[482]

The term, "private", comes from the Latin word, "*privatus*", meaning "withdrawn from public life", and from "*privus"*, meaning "single, individual".[483] "Privacy" comes from the Latin words, "*sōlitūdō, sēcrētum*", meaning "solitariness, secret".[484]

The term "privacy" is enigmatic and elusive. No single definition can encapsulate the entire concept. As a result, it is hardly surprising that there are several social theories attempting to provide an interpretation of what privacy means and what rights and interests it protects. The inevitable result is frustration in trying to understand and define privacy. However, with each new attempt to demystify the concept, there is a potential for further confusion given the accumulation of divergent approaches. This frustration experienced by theorists has led to several theorists agreeing that "privacy is a concept in disarray".[485] Indeed, the struggle to answer the question, "What is privacy?" presents several challenges to the theoretical field.

In Chapter 2, I delved into different theories of surveillance in order to understand the nature of electronic surveillance, and explored theories that are relevant to the employment context both inside and outside the workplace. I examined two sides of a

---

[482] Glenn Greenwald, *No Place to Hide* (Toronto: Signal, 2014) at 172.
[483] Angus Stenson, ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010) *sub verbo* "private".
[484] Grocyn Lecturer & James Morwood, eds, *Oxford Latin Desk Dictionary* (Oxford: Oxford University Press, 2005) *sub verbo* "privacy".
[485] Daniel J Solove, "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477 at 477 [Solove, "Taxonomy].

coin (with the ubiquity of surveillance on the one side and surveillance inside the workplace on the other) with a panoptic rim, and did so using a capitalist surveillance theoretical lens.

In this Chapter, I plan to examine views of what privacy means in a more philosophical way.

There are two main categories of privacy theories—reductionist and non-reductionist—and my goal is to explain why most of these privacy theories are problematic and indicate why I prefer one particular theory of privacy.

More specifically, the reductionist theorists I discuss either understand privacy as a cluster-of-rights, or use an economic perspective when conceptualizing privacy. On the other hand, the non-reductionist theories variously regard the invasion of privacy as a tort, or adopt a feminist legal theory of privacy, or view privacy primarily involving control-over-information, or adopt a pragmatic contextual approach to privacy.

The theory of privacy that I prefer is the dignity/human rights approach to privacy. This perspective provides an appropriate understanding of privacy and allows for a purposive interpretation that does not ignore the interests of the most vulnerable citizens. When examining privacy with this lens, the interpretation of privacy provisions and workplace privacy cases will help me draft a more effective workplace privacy regime.

It is important to understand all of the selected theories in order to build a rich foundation for vibrant socio-legal analyses in Chapters 4 and 5. In fact, I will be relying on all of these conceptualizations throughout the analyses to some extent in order to understand what is being protected when creating the new workplace privacy regime.

To that end, the purpose of this Chapter is to review and critique selected different theoretical approaches to privacy using a dignity/human rights theoretical perspective on privacy.

3.1 The Problem with Most Privacy Theories

The problems associated with the two types of theories, reductionist and non-reductionist theories, are set out below.

3.1.1 Reductionist Theories

Reductionists are critical of singling out privacy and see no reason for treating it as particularly special.

For example, Judith Jarvis Thomson believes that there is no unique right to privacy that requires separate protection because there is no part of privacy that is not covered by some other right.[486] In her overly-skeptical discussion of privacy, she attempts to determine whether every so-called violation of the right to privacy is that, or is instead the violation of some other right.[487] In order to accomplish this task, she uses a hypothetical example, and explains that what is happening when a person observes a quiet fight behind closed windows using an amplifier is indeed a violation of a right, but not that of the right to privacy; rather, it is a violation of the right not to be listened to, which is one of the rights included in the "right over the person".[488]

Thomson is unconvincing when she states that the privacy cluster-of-rights is not distinct because it overlaps with the cluster-of-rights dealing with owning property.[489] She suggests that there is nothing detectable that needs to be isolated because everything about privacy is encapsulated in a different set of rights. Thomson assumes that all aspects of privacy are the same as those dealing with property; however, there are unique features that pertain to privacy that do not involve the protection of property—but Thomson dismisses this idea without even exploring it. It would have been useful for Thomson to attempt to isolate some features that are unique to both privacy and property protection, in addition to identifying any overlapping features—before making this kind of assertion.

---

[486] Judith Jarvis Thomson, "The Right to Privacy" (1975) 4:4 Philosophy and Public Affairs 295 at 310.
[487] *Ibid* at 295.
[488] *Ibid* at 305.
[489] *Ibid* at 306.

Thomson puts forth a theory that is problematic. On one hand, Thomson contends that there are no rights in the right to privacy cluster that are not also in some other rights cluster, and on other hand, she maintains that the term, privacy, is unclear and it is not known what would be included in this privacy cluster.[490] Thomson then points to other factors that are involved with privacy, including rights to life, liberty, property, and the right to not to be harmed.[491] In fact, Thomson suggests since every right in the right to privacy cluster is also in some other right cluster, there is no need to find what is in common to all rights in the right to privacy cluster and no need to settle disputes about boundaries.[492] She argues that wrongs involving privacy can be explained without ever mentioning the word, privacy, and concludes that a person need only ask whether an act is a violation of any other right, and if not, whether the act really violates a right at all.[493] The problem with this idea, simply put, is that there is no way of confirming the conclusion that everything about privacy is covered under some other cluster-of-rights.

But most disconcerting, Thomson characterizes privacy as "derivative"[494] and evades the necessary consideration of what privacy really entails, and in so doing, she neglects to consider the fundamental nature and importance of privacy. It is not acceptable to argue that, since every right in the right to privacy cluster is also in some other right cluster, there is no need to bother analyzing privacy. Concluding that wrongs involving privacy can be explained without ever mentioning the word "privacy" is like asking a question about the rain without discussing the weather. This analysis is far too dismissive of the essential nature of privacy; this is because privacy is not covered by any other right. Thomson fails to consider the dignity and self-respect of individuals who are in need of real privacy protection—with a right to privacy.

Amy L. Peikoff also adopts a reductionist approach to privacy. She agrees with Thomson and maintains that there is no legal right to privacy since the legal protection of privacy is

---

[490] *Ibid* at 310.
[491] *Ibid* at 312.
[492] *Ibid* at 312–313.
[493] *Ibid* at 313–314.
[494] *Ibid* at 312.

grounded in other rights to liberty, property and contract.[495] She goes even further than Thomson and rejects the idea of privacy as a legal concept, claiming that it is not even a derivative legal concept.[496] To Peikoff, any law protecting privacy would be subjective and unjust, and laws directed specifically at invasions of privacy would erode fundamental rights to liberty and property.[497] Consequently, she recommends a move toward the jurisprudence of liberty, property, and contract so long as these changes provide a net increase in the protection of individual rights.[498] Moreover, Peikoff asserts that the reductionist defence lies in showing why property and liberty are fundamental compared to privacy, and also showing why recognizing a distinct legal right to privacy would be improper.[499]

Peikoff's discussion is just as flawed as Thomson's because it fails to truly appreciate the value of privacy or consider privacy as something in need of separate protection. Rather, Peikoff frames privacy as a villain that stands in the way of fundamental rights of liberty, property and contract. Harsher than Thomson, Peikoff assumes that anything related to the idea of a right of privacy would be subjective and therefore unjust. Thus, it is decided that a subjective analysis that considers the surrounding circumstances is something negative and undesirable. But this conclusion fails to take into account how important it is to have some flexibility in order to balance interests and evolve with society when it comes to understanding fundamental values such as privacy. Peikoff simply does not see privacy except as an obstacle that interferes with liberty, property, and contract.

Another reductionist, the economic theorist and modern utilitarian Richard A. Posner, believes that privacy involves the withholding or concealing of information.[500] Using an

---

[495] Amy L Peikoff, "Beyond Reductionism: Reconsidering the Right to Privacy" (2008) 3 NYU J L & Liberty 1 at 5 [Peikoff, "Beyond Reductionism"].
[496] *Ibid*.
[497] *Ibid* at 20–46.
[498] *Ibid* at 46–47.
[499] Amy Peikoff, "The Right to Privacy: Contemporary Reductionists and Their Critics" (2006) 13 Va J Soc Pol'y & L 474 at 534 [Peikoff, "Contemporary Reductionists"].
[500] Richard A Posner, "The Right of Privacy" (1977-1978) 12 Ga L Rev 393 at 393. Theorists have classified Posner as a reductionist. See Peikoff, "Contemporary Reductionists", *supra* note 499 at 551. Economic legal analysis is viewed as a subset or a modern form of positivism/utilitarianism. See Krister Bykvist, *Utilitarianism: A Guide for the Perplexed* (London: Continuum International Publishing Group,

economic perspective, he focuses on the demand for private information and views it as something that can create opportunities for gain by the demander.[501]

That said, even Posner acknowledges that framing privacy in this way presents opportunities for exploitation through misrepresentation.[502] One may reject his ideas about privacy since there is no discussion about the circumstances that might surround the demand for private information or the holder of information. One may also wonder how unequal bargaining power affects this analysis, and how the analysis is affected where third parties experience costs while others gain. There is certainly no discussion about how this conceptualization of privacy affects vulnerable parties.

Posner argues that the process of voluntary exchange of personal information ensures that the information is put to its most valuable use, and the attractiveness of the solution depends on the nature and provenance of the information, along with transaction costs.[503]

But even Posner can see that at some point nondisclosure becomes fraud, and this can take place when a transacting party has crossed the line and the information that party seeks to conceal is a product of significant investment.[504] One may find that, practically speaking, there currently are instances where individuals provide their information in exchange for some benefit. However, one may denounce the idea of treating personal information as a commodity and using it as a pawn in a data exchange for value. One may wonder whether persons appreciate what has been given up and whether they are able to appreciate how the information can be put to its most valuable use. Unquestionably, when treating data as a commodity like this, there is a large potential for exploitation of the weaker party.

2010) at 1; J W Harris, *Legal Philosophies* (London: Butterworths & Co (Publishers) Ltd, 1980) at 24; Raymond Wacks, *Philosophy of Law: A Very Short Introduction* (Oxford: Oxford University press, 2014) at 25−48, 76−83.

[501] Posner, *supra* note 500 at 394.

[502] *Ibid*.

[503] *Ibid*.

[504] *Ibid* at 398.

What is most troubling is that Posner argues that very few people want to be left alone; rather, he says that they want to manipulate the world around them by selective disclosure of facts about themselves.[505] One difficulty with this approach is that many do not agree that the main goal of seeking privacy is to manipulate others in the world around them. Another difficulty is that the approach neglects to appreciate that there are several benefits to privacy, and hence, there are several motivators. For example, a person may want privacy in order to derive creative benefits or solve a problem and to be free to experiment and generate alternatives in a safe place. There is simply no acknowledgment that privacy fulfills the goal of maintaining dignity and self-respect and preserving aspects of humanity.

Although Posner contends that there is a difference between prying by means of casual interrogation versus electronic surveillance, he problematically focuses on the narrow topics of efficiency and transaction costs.[506] That is, Posner maintains that conversation is more costly because of the external effects, and the increased costs would result in less effective communication since people would be more guarded in their speech.[507] Indeed, the main concern with this theory is about efficiency—Posner argues that the trend toward expanding the privacy protections of individuals while contracting interests of organizations is inefficient.[508]

One may frame this analysis as something that appears to be all about hidden agendas to hide information, manipulate others, or to get something to increase value and efficiency. Using this reasoning, the protection of privacy becomes a nonpriority because it does not maximize wealth in society. Posner asserts that privacy should only be protected when access to the information would reduce its value. The theory promotes transparency as the default position, with privacy only becoming worthwhile if it can increase opportunities for gain without increasing costs.

---

[505] *Ibid* at 400.
[506] *Ibid* at 401.
[507] *Ibid*.
[508] *Ibid*.

And one may insist that this economic approach is irresponsible since long-term consequences and a consideration of the circumstances are completely ignored; for the sake of short-term gains, individuals may be tempted to surrender pieces of information that could be used in ways they do not understand at the time. This puts the weaker party at risk of being exploited and left behind. It also neglects to even consider the fundamental nature of privacy and its essential value when it comes to promoting dignity and self-respect. Simply put, on Posner's view privacy is treated as a means to various other ends, and as something that can be interfered with or violated if doing so is necessary to protect other, more valuable goals. This is problematic.

James B. Rule agrees with Posner and uses a similar economic analysis of privacy.[509] In fact, he believes that the rise of cyberspace has led to new sources and possibilities for appropriation and use of personal information in several spheres of life, given all of the ways of knowing who people are, what their interests and susceptibilities are, what they are willing to buy, and how much they can be expected to pay.[510] Rule proposes a new right over the commercial exploitation of personal information on oneself.[511] In fact, he maintains that individual ownership of the right to commercialize data on oneself, properly implemented, creates broad and meaningful possibilities for ordinary private citizens to curtail commercial use of their data or to shape the character of such use.[512] Rule contends that this brings clarity because there is no commercial exploitation of personal data allowed without the permission of the individual concerned.[513]

Rule cites what is sometimes called the total utility principle: the best use of such personal data is the highest use, or the one commanding the highest price in some sort of open market.[514] Clearly, the economic theory evolves from the classic positivism/utilitarian theory aimed at making some people better off and no one worse

---

[509] James B Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" (2004) 54 U Toronto L J 183.
[510] *Ibid* at 183–184.
[511] *Ibid* at 185.
[512] *Ibid*.
[513] *Ibid* at 185–186.
[514] *Ibid* at 190.

off, to generate an overall societal improvement.[515] The principle of utility is: "the greatest happiness of the greatest number".[516] The reasoning process is that one must: examine the available options for action at the time, identify the outcomes of those actions, and then evaluate each outcome by how much well-being it contains, and the best outcome is the outcome that contains the greatest total sum of well-being to provide clarity, simplicity, explanatory power, coherence, and consistent prescriptions.[517] In fact, the economic theory is derived from the positivism/utilitarian theory.[518]

What is most disquieting about both the utilitarian and economic theory is that they carry significant dangers, especially for the most vulnerable in society. In exchange for certainty and simplicity, weaker individuals may not benefit and could even become subject to serious exploitation. Essentially, using utilitarian principles could lead to pleasing the highest number of individuals, and failing to take into account the dignity and self-respect of the most vulnerable citizens. There is a mistaken assumption made in this theory that individuals are able to make competent decisions about how to maximize their own value and the value of their information. There is simply no discussion about how to empower the weaker individuals during these data exchanges aimed at maximizing value—it is merely accepted that they will be left behind.

In short, my criticism of reductionist theories of privacy is that they fail to truly grapple with or address what makes privacy, or the right to privacy, unique and important. Thomson and Peikoff suggest that the right to privacy is really nothing over and above the right to one's person, property, or liberty, or the right not to have one's person or property damaged or harmed; while Posner and Rule view the right to privacy as a barrier

---

[515] Bykvist, *supra* note 500 at 1.
[516] Harris *supra* note 500 at 24, 36. See also Ben Eggleston & Dale E Miller, *The Cambridge Companion to Utilitarianism* (Cambridge: Cambridge University press, 2014); Thomas Hobbes, *Leviathan*, ed by C B MacPherson (London: Penguin Looks Ltd, 1985); John Stuart Mill, *The Basic Writings of John Stuart Mill*, ed by Dale E Miller (New York: The Modern Library, 2002); Jan Narveson, *Morality and Utility* (Baltimore: The Johns Hopkins Press, 1967).
[517] Bykvist, *supra* note 500 at 16–17, 22–24.
[518] Eggleston & Miller, *supra* note 516 at 42–44; Jon L Mills, *Privacy: The Lost Right* (Oxford: Oxford University press, 2008) at 70–72.

to the efficient allocation of resources. What all these approaches share in common is a skepticism about the coherence and utility of the concept of privacy.

3.1.2 Non-Reductionist Theories

Non-reductionist theorists believe that there is some coherent value in privacy, although they disagree on how the value is understood, conceptualized, and operationalized.

Samuel D. Warren and Louis D. Brandeis' 1890 article is the first of its kind to suggest that the law must recognize the right to be let alone.[519] Warren and Brandeis assert that there should be a law that acknowledges the right to privacy to protect people from the growing interference of the press to address serious concerns about instantaneous photographs, newspapers and the circulation of portraits.[520] They maintain that numerous mechanical devices threaten to make good the prediction: "what is whispered in the closet shall be proclaimed from the house-tops".[521] In describing mechanical devices as a threat, it is clear that Warren and Brandeis are expressing a dystopian perspective concerning technology, suggesting that technology can threaten the established ways of life and can even be viewed as a regressive force.[522] This, in turn, strongly influences their perspective regarding the value and protection of privacy. For instance, they describe the invasion of privacy by the newspapers as "evil", state that the press is overstepping in every direction the obvious bounds of propriety and of "decency", and express distaste regarding personal gossip attaining the "dignity of print".[523] Invasions of privacy are considered unquestionably unethical, and appear to be rooted in the use of technology. These types of publications causing injury are considered an "intolerable abuse".[524] Ultimately, Warren and Brandeis argue that if one were to examine solely the

---

[519] Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193. It is important to note that it was Thomas M Cooley who coined the phrase, "right to be let alone" as far back as 1888. See Thomas M Cooley, *A Treatise on the Law of Torts on the Wrongs which arise Independent of Contract,* 2nd ed (Chicago: Callaghan and Company, 1888) at 29. That said, it was Warren and Brandeis who gave original meaning to this phrase.
[520] Warren & Brandeis, *supra* note 519 at 193-195.
[521] *Ibid* at 195.
[522] Anabel Quan-Haase, *Technology & Society Social Networks, Power, and Inequality* (Oxford: Oxford University Press, 2016) at 43 [Quan-Haase, "Technology"].
[523] Warren & Brandeis, *supra* note 519 at 195–196.
[524] *Ibid* at 210.

right to privacy, one would be left with a more general right to the immunity of the person, or the right to one's "inviolate personality".[525]

Here is the first problem: Warren and Brandeis mistakenly use ambiguous words and phrases, such as "right to liberty", "immunity of the person", and "inviolate personality" which leads to a conceptualization of privacy that is overly broad, unclear regarding reconciling competing interests, and lacking in precision. It is unclear what these terms mean, yet the authors do not provide any explanation—this is critical given that the terms form the foundation of their argument. For instance, the "right to liberty" does not explain what interests are contemplated; surely, it cannot mean freedom to do anything a person wants to do, and yet there must be some limit to what is protected under the umbrella of the right to privacy. One may wonder whether a person's privacy can be protected even when that person is doing something that is considered by society to be ethically unsound. Similarly, another aspect that weakens the argument is that it is not clear how privacy could be protected in circumstances where there are competing liberty interests, and there is no assistance on how to conduct this analysis. The dilemma of how to resolve competing interests remains unresolved in this analysis. Indeed, Warren and Brandeis admit the inevitable difficulty in identifying where to draw the line.[526] Additionally, "immunity of the person" and "inviolate personality", make no sense in the context in which they are used. It is difficult to understand what the authors mean because the argument is based on puzzling phrases that read more like a set of riddles rather than a clear logical argument. Dictionaries are not helpful: "immunity" is defined as "officially granted exemption from legal proceedings or liability", or "lack of susceptibility, especially to something unwelcome or harmful", from the Latin, "*immunitas*" and "*immunis*", meaning "exempt from charge".[527] Also, "inviolate" is defined as "free or safe from injury or violation", from the Latin, "*inviolatus*", meaning "not violate".[528] One may question exactly what the authors have reduced privacy to.

---

[525] *Ibid* at 205–207.
[526] *Ibid* at 214–219.
[527] Stenson, *supra* note 483 at *sub verbo* "immunity".
[528] *Ibid* at *sub verbo* "inviolate".

Here is the second problem: the strong language, the dystopian view of technology, and the link created between morality, justice, and privacy results in a view of privacy that is anything but neutral, giving the concept of privacy positive value without clearly explaining why. While I agree that there is value to privacy, I believe that it is important to provide a reason that justifies why there is such value. In Warren and Brandeis' article, there is no elucidation of their reasoning in this regard. In light of the strong tone of the article, it is clear there is something causing the reaction, but nothing is particularly explicated concerning what the value of privacy actually is. Indeed, there is an absence of a well-articulated discussion regarding the benefits of privacy, why individuals would want it, and how dignity and self-respect can be maintained by providing it. Notwithstanding the rigorous language used in this article, there is no discussion about how the weaker, more vulnerable, individuals they are aiming to defend are potentially taken advantage of with these "evil" and threatening technological devices as described by Warren and Brandeis.

William L. Prosser does not agree with Warren and Brandeis and provides a different take on torts involving invasions of privacy.[529] He maintains that the invasion of privacy covers intrusion upon the plaintiff's solitude; publicity given to his or her name or likeness or to private information about him; placing him or her in a false light in the public eye; and commercial appropriation of elements of his or her personality.[530] Prosser believes that the right to privacy is subject to a privilege to publish matters of news value or of public interest of a legitimate kind.[531] Not only does he argue that there are four torts involving the invasion of privacy without any justification for his choices, but he also does not provide any clarification about what he considers as the exception, involving matters that are of news value or of public interest of a legitimate kind.

Prosser takes a cynical approach when referring to Warren and Brandeis' article and characterizes it as an outstanding (and not in a good way) illustration of the influence of

---

[529] William L Prosser, *Handbook of The Law of Torts,* 2nd ed (St Paul Minnesota: West Publishing Co, 1955).
[530] *Ibid* at 635.
[531] *Ibid*.

legal periodicals upon the courts.[532] Prosser argues that in reality, the right to privacy appears to be a complex of four distinct wrongs, which have little in common except that each is an interference with the plaintiff's right "to be let alone".[533] If matters are examined more closely, it may be concluded that the success of this argument is highly questionable as it is puzzling that Prosser compartmentalizes aspects of privacy into four categories consisting of traditional forms of protection and then claims that they are not related. There is a complete failure to appreciate that privacy is a fundamental right that individuals enjoy simply by virtue of being human. This concept cannot be divided and placed into separate categories.

What is most troubling about this conceptualization of privacy is that Prosser is reluctant to accept that there is a separate, freestanding right of privacy. In fact, he appears to be most concerned about the importance of privilege to publish, and the unquestionable freedom of the press—he asserts that those who put themselves in the public eye, including actors, inventors, explorers, or public officers, have no right to complain of any publicity which reasonably bears on their activity.[534] Even individuals who live more public lives are still human, and deserve to be protected from powerful parties who have the potential to abuse monitoring power—they are still worthy of protection. That said, Prosser states that the publishing privilege is not unlimited and there is a line, but the line is difficult to draw.[535] Yet, when he draws the line, he only stops at outrageous behaviour that would outrage the common decency beyond what the public will tolerate: unless a person is liable for intentional infliction of mental suffering, the plaintiff would be expected to endure all other privacy intrusions for the sake of sensational reporting.[536] This fragmented approach seems more declaratory than analytical, and it also takes an extremely narrow view of privacy in that the right of privacy is only protected in rare, exceptional cases. Privacy is given a very low value, and appears to be outweighed by ideas of security and other interests such as freedom of expression in almost every case.

---

[532] *Ibid*.
[533] *Ibid* at 637.
[534] *Ibid.*
[535] *Ibid* at 643–644.
[536] *Ibid*.

In this extremely skewed analysis, it is clear that the dignity and self-respect of individuals are not a priority.

Contrastingly, various feminist legal theorists provide a compelling perspective on privacy that highlights some of the considerations that tend to be overlooked in other analyses of privacy. For example, Judith Wagner DeCew asserts that the main concern of feminist scholars is about the darker side of privacy and the use of privacy as a shield to conceal negative treatment of women, including domination, degradation, and abuse.[537] Furthermore, according to the feminist perspective, the distinction between the public and private realms has the effect of allowing the private realm to be free from scrutiny, and by completely refraining from getting involved in the private domain, the State allows repression and physical harm to be perpetuated.[538] Certainly, this approach sheds light on a minority perspective and signals that there can be a danger in having an overly broad and categorical approach to privacy.

In a balanced analysis, DeCew states that while it is important to acknowledge the danger of privacy acting as a shield for abuse, it is unacceptable to reject privacy completely just because of the potential for harm done in private.[539] DeCew maintains that allowing everything to be public and transparent, leaving the domestic sphere open to complete scrutiny, is unworkable, and as such, it is not appropriate to simply collapse the public/private dichotomy.[540] In fact, DeCew suggests that this type of transparency is unacceptable and even dangerous because it grants excessive power to the State.[541] Using a broader conception of privacy, DeCew contends that it is possible to appreciate the pitfalls of the dichotomy, while still retaining a meaningful concept of privacy.[542] She

---

[537] Judith Wagner DeCew, *In Pursuit of Privacy, Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997) at 81 [DeCew, "In Pursuit"].
[538] DeCew, Judith, "Privacy" (18 January 2018), online: *Stanford Encyclopedia of Philosophy* <https://plato.stanford.edu/entries/privacy/> [DeCew, "Privacy"].
[539] *Ibid*.
[540] *Ibid*.
[541] DeCew, "In Pursuit", *supra* note 537at 94.
[542] *Ibid*.

argues that privacy is not an absolute value, but can be viewed as the default, requiring government and others to justify their need to intrude.[543]

Similarly, Carole Pateman agrees that the public/private dichotomy is central to almost two centuries of feminist writing and political struggle, and is essentially what the movement is all about.[544] She explains why feminists reject liberal conceptions of the private and public and view the social structure of liberalism as the political problem, not the starting point, from which equal rights can be claimed.[545] In fact, Pateman states that feminists stand alone when raising the generally neglected problem of the patriarchal character of liberalism.[546] Ultimately, Pateman posits that a proper understanding of liberal social life is possible only when it is accepted that the two spheres (the private domestic and the public civil society) that are separate and opposed, become inextricably interrelated.[547] Pateman believes that, presently, women have been almost completely excluded from public life, or alternatively, they have been included in patriarchal ways.[548]

Although DeCew and Pateman highlight the dark side of privacy, they do not provide any solutions regarding how public and private spheres can coexist in an interrelated manner. In modern society, it appears to be possible to have a right to privacy where these spheres can exist in an interrelated manner, so that there is more equality in both spheres. In more progressive households, men and women share in the domestic work, and, both men and women work in the public sphere in paid employment. However, at this point, it cannot be said that what Pateman is suggesting has actually taken place to the extent that she envisions given the different allocations of work, gender wage gap, and glass ceiling effects.

---

[543] Judith Wagner DeCew, "Privacy" in Andrei Marmor, ed, *The Routledge Companion to Philosophy of Law* (New York: Routledge, 2012) 584 at 597 [DeCew, "Routledge Privacy Paper"].
[544] Carole Pateman, "Feminist Critiques of the Public/Private Dichotomy" in Susan Moller Okin & Jane Mansbridge, eds, *Feminism* (Cambridge: Edward Elgar Publishing Company, 1994) vol 1, 327 at 327.
[545] *Ibid*.
[546] *Ibid* at 328.
[547] *Ibid* at 330–331.
[548] *Ibid*.

Given the narrow focus, what is especially missing with this theory is a discussion about how fundamental privacy can be in this context. In their attempt to argue for transparency to expose the dark side of privacy, whether it is complete or partial, there is a consequent failure to discuss any potential value of privacy in a meaningful way.

Some feminist theorists are more aggressive when exploring the nature of a right to privacy and its impact on the private and public spheres. For instance, Catherine A MacKinnon, a radical feminist, asserts that over and over again that the State protects male power by ensuring male control over women at every level.[549] Further, she argues that women are kept socially dependent on men and are kept poor—the law merely stands passively by reflecting the scene.[550] MacKinnon states that the law of privacy treats the private sphere as the sphere of personal freedom; for men, this is the case, but for women, the private sphere is the distinctive sphere of intimate violation and abuse which is neither free nor personal.[551] According to MacKinnon, men enjoy personal freedom, whereas women are subject to collective subordination since public repression masquerades as private freedom.[552] MacKinnon argues that privacy law assumes women in the private sphere have the same privacy that men do, just as equality law assumes that women are essentially equal to men in the private sphere.[553] In her view, this is the problem, because realistically speaking, it is not the case.[554]

MacKinnon maintains that while the law of privacy proposes to guarantee individual bodily integrity, personal exercise of moral intelligence, and freedom of intimacy, women's rights to access those values have not been guaranteed.[555] Yet the privacy ideal holds: as long as the public does not interfere, autonomous individuals interact freely and equally.[556] To MacKinnon, for women, the measure of intimacy has been the measure of

---

[549] Catherine A MacKinnon, *Toward a Feminist Theory of the State* (Cambridge: Harvard University Press, 1989) at 167–168.
[550] *Ibid* at 168.
[551] *Ibid*.
[552] *Ibid* at 169.
[553] *Ibid*.
[554] *Ibid*.
[555] *Ibid.*
[556] *Ibid* at 190.

oppression, so feminism has had to "explode the private".[557] Essentially, MacKinnon asserts that women have no privacy to lose or to guarantee.[558]

In one sense, it is understandable that MacKinnon would wish to reject the private/public distinction, given that the distinction perpetuates the mistreatment suffered by women. In this way, she could be preventing or at least minimizing the darker side of privacy. However, MacKinnon then goes on to argue that women do not benefit either way from privacy protections because they have no privacy to lose or to guarantee in light of the inequality that exists. If this is the case, it is unclear why the private sphere would have to be exploded. One may object to her arguments and point to their confusing and impractical nature; one may also object to the idea of "exploding" an entire sphere of life. If the goal is to eliminate the private sphere so that there is no distinction between private and public, the end result will be complete transparency. There are dangers associated with complete transparency, opening the door to further potential for exploitation. This may help prevent the darker side of privacy because any previously hidden abuse could be revealed, but this complete transparency would lead to everything being subject to intervention and scrutiny. There is a failure to acknowledge the fundamental value of privacy.

One may raise a further objection to MacKinnon's use of combative language when she indicates that the right to privacy looks like an injury presented as a gift, a sword in men's hands presented as the shield in women's hands.[559] She criticizes privacy law as isolating women from each other and from public recourse, and makes this classic statement: the right to privacy is "a right of men "to be let alone" to oppress women one at a time".[560]As one of the pioneers of the feminist perspective, she may believe that this is the only way to make the point. In fact, it is common for social movements to begin and gain momentum with extreme leaders, and gradually progress with more tempered

---

[557] *Ibid* at 191.
[558] *Ibid.*
[559] *Ibid* at 191.
[560] *Ibid* at 194.

leaders using compromise.[561] In the end, MacKinnon leaves us with no real solution, and there is no guarantee that collapsing the spheres would rectify any of the problems she cites, since there are situations where individuals are aware of one's mistreatment, but they do not act or influence a change of any kind. Ultimately, MacKinnon's conflicting arguments leave us to wonder how they can be reconciled, and whether it is even possible to have privacy free from the darker side of privacy.

Let me pause here to recap what I have discussed to this point. I have so far examined two types of non-reductionist theories. The first set of theories involved viewing privacy as the tort of invasion of privacy, as explained by Warren and Brandeis and also Prosser. The second group of theories concerned various feminist approaches to privacy, where theorists such as DeCew, Pateman, and MacKinnon highlight the dark side of privacy. Now I will discuss theories pertaining to the control-over-information perspective.

Theorists who view privacy as control-over-information provide a unified description and account of privacy. For example, Ruth Gavison argues that it is important to ensure that there is a neutral concept of privacy that can enable us to identify when a loss of privacy has occurred; privacy has coherence as a value; and privacy is a concept that is useful in legal contexts so that it enables us to identify occasions calling for legal protection.[562] Gavison concludes that privacy is coherent and useful in these three situations, and that losses of privacy, invasions of privacy, and actionable violations of privacy are related because each is a subset of the previous category.[563]

In fact, Gavison states that our interest in privacy is related to our concern over our accessibility to others and the extent to which we are known to others; the extent to which others have physical access to us; and the extent to which we are the subject of others' attention.[564] To her, viewing privacy as limited accessibility enables the identification of

---

[561] Adam M Grant, *Originals: How Non-Conformists Move the World* (New York: Viking, 2016) at 117–145.
[562] Ruth Gavison, "Privacy and the Limits of the Law" in David Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 346 at 347.
[563] *Ibid.*
[564] *Ibid.*

when losses of privacy occur—the reasons why we claim privacy involves the function that privacy has in our lives, including the promotion of liberty, autonomy, selfhood, and human relations.[565] Gavison warns however, that since privacy is seldom protecting an interest in absence of some other interest, the danger is that one might conclude that privacy is not an important value in itself.[566] However, Gavison states that, when considering the meaning and function of privacy, privacy is a value that is in need of protection.[567]

What is especially unique in Gavison's approach is that she proposes that individuals enjoy perfect privacy when they are completely inaccessible to others, with no one having information about the person, no one paying any attention to the person, and no one having any physical access to the person.[568] Gavison states however, that perfect privacy is impossible in any society.[569] A loss of privacy takes place as others obtain information about the person (loss of secrecy), pay attention to the person (loss of anonymity), or gain access to the person (loss of solitude).[570] According to Gavison, secrecy, anonymity, and solitude are distinct but interrelated.[571]

Several other theorists agree with Gavison. Anita Allen, for example, argues that privacy denotes a degree of inaccessibility of persons, their mental state, and information about them to the senses and surveillance devices of others. [572] According to Allen, in order to say that a person is enjoying privacy, that person must be beyond the range of others' senses and any devices that can enhance, reveal, trace, or record human conduct, thought, belief, or emotion.[573] Alan F. Westin argues that privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent

---

[565] *Ibid.*
[566] *Ibid* at 348.
[567] *Ibid.*
[568] *Ibid* at 350.
[569] *Ibid* at 350–351.
[570] *Ibid.*
[571] *Ibid.*
[572] Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (New Jersey: Rowman & Littlefield, 1988) at 3.
[573] *Ibid* at 15.

information about them is communicated to others.[574] Westin asserts that privacy is the voluntary and temporary withdrawal of a person from the general society to physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.[575] He states that individuals are continually engaged in a personal adjustment process where they balance the desire for privacy with the desire for disclosure and communication of themselves to others in light of the environmental conditions and social norms set by society in which the person lives.[576] To Westin, individuals go through this process in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets to enforce social norms.[577]

Similarly, W. A. Parent maintains that privacy is the condition of not having undocumented personal information about oneself known by others.[578] Parent states that personal information consists of facts about a person which most individuals in a given time do not want widely known about themselves.[579] However, since some people are more sensitive than others and may take extreme measures to make sure people do not find out more benign information, Parent suggests that personal information consists of facts that most people in a given society choose not to reveal about themselves or of facts about which particular individuals are acutely sensitive and therefore do not choose to reveal about themselves, even if most persons do not care if these facts are widely known.[580] Likewise, Raymond Wacks argues that the best account of privacy is limited accessibility, a cluster of three related but independent components: secrecy (information known about an individual); anonymity (attention paid to an individual); and solitude (physical access to an individual).[581] Wacks maintains that the essence of his argument is that at the center of the concern about privacy is the use and misuse of personal

---

[574] Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1968) at 7.
[575] *Ibid.*
[576] *Ibid.*
[577] *Ibid.*
[578] W A Parent, "A New Definition of Privacy for the Law" (1983) 2 Law and Philosophy 305 at 306.
[579] *Ibid* at 306–307.
[580] *Ibid.*
[581] Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989) at 15–16.

information about an individual.[582] Ultimately, Wacks defines personal information as facts, communications, or opinions which relate to the individual and which it would be reasonable to expect them to regard as intimate or sensitive and therefore to want to withhold or at least restrict their collection, use or circulation.[583]

Although this theory is a more modern take on personal information in light of technology, accepts that there cannot realistically be complete privacy, and recognizes the importance of balancing interests in the circumstances, there are some shortcomings. Here is one shortcoming: there is a failure to specifically identify types of information over which individuals have control, making the theory somewhat vague. Here is another shortcoming: there are issues regarding how certain words are defined, such as control and personal information. Here is another shortcoming: it is unclear how this information that is controlled can have a realistic limit without being overly broad, and one may wonder whether all the information about a person may end up being within a person's control, especially in the case of sensitive individuals.

But the most bewildering shortcoming of the control-over-information theories is this: it is unclear how this theory differs from the economic theory given that personal information can be viewed as any other commodity and used as a tool to achieve something, especially in the context of technology. In particular, a person could actually make decisions in the spirit of controlling their information, but incidentally or purposely exploit their information to gain value in a transaction. This would lead to the same problems that were discussed when criticizing the economic theory of privacy. For example, all of the dangers of putting weaker individuals at risk of exploitation would be present. Most troubling would be that privacy would be used as a means to get something, manipulate something, or gain value in some way at the expense of the dignity and self-respect of the most vulnerable citizens. Simply put, some individuals may remain exposed since they may not be in a position make wise decisions regarding how their information will be used in a data transaction to gain value and efficiency.

---

[582] *Ibid* at 20.
[583] *Ibid* at 26.

Lastly, the pragmatic, contextual approach attempts to be realistic, flexible, and open to maintaining contextual integrity. Andrew McStay explains that theorists who take a pragmatic, contextual view of privacy attempt to remove binary terms such as public/private.[584] Instead, they focus on expressing privacy with respect to appropriateness, context, the type and nature of information, and with whom information is being shared.[585] In fact, the main feature of the pragmatic, contextual point of view is that people do not require complete privacy, and different norms apply in different circumstances.[586] McStay describes the contextual approach as an attempt to deal with the fact that privacy matters are informationally and technologically complex.[587] He points out that recognition of situation dependency allows for flexibility that is not found in the absolutes of the other privacy theories.[588]

While theorists who adopt non-reductionist approaches clearly have good intentions and are trying, in a pragmatic and realistic way to disentangle the conceptual mess of privacy, they unfortunately cause a series of unintended consequences. In particular, they break the concept of privacy using explanations that are not helpful—the explications are overly complicated, shapeless, and without an anchor to support a meaningful understanding of privacy or how to go about assessing competing claims.

Simply put, there is nothing undergirding their analyses. There is no appreciation of the value of privacy because it shifts back and forth, depending on the direction in which the wind is blowing. Ultimately, these sorts of non-reductionist theories provide no solid understanding of what privacy is, and consequently, no north star to guide us.

---

[584] Andrew McStay, *Privacy and Philosophy* (New York: Peter Lang Publishing Inc, 2014) at 50.
[585] *Ibid*.
[586] *Ibid*.
[587] *Ibid*.
[588] *Ibid* at 53. See also Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010) at 1−2, 103, 129−134, 231–233; Daniel J Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008) at 8–38, 70–74 [Solove, "Understanding Privacy"].

3.2 Proceeding with the Dignity/Human Rights Approach

What is needed, in short, is an account of privacy that (1) recognizes privacy as a freestanding right or concept, not reducible to rights to persons or property, or subject to limitation in the service of economic goals; and that (2) indicates what makes privacy important. In my view the dignity/human rights approach to privacy can accomplish both of these tasks. At its core, this approach is a more sophisticated version of the right to be let alone—the main point being that individuals are to be treated as ends in themselves rather than as means to furthering another person's or society's goals.[589] In fact, the idea that invasions of privacy constitute offenses to dignity can be traced back to Kantian times.[590]

One strong advocate for the dignity/human rights approach to privacy is Edward J. Bloustein. His method of highlighting the importance of dignity in respect to privacy is to criticize Prosser, the theorist advancing the claim that privacy should be conceptualized as a tort.[591] Essentially, Bloustein rejects Prosser's analysis and argues that assaults on privacy have been transmuted into the torts of defamation, infliction of mental stress, and misappropriation—using this analysis, there is no new tort of invasion of privacy, but only new ways of committing old torts.[592] Bloustein asserts that Prosser's analysis leads to the social value of privacy becoming a composite of the value our society places on protecting mental tranquility, reputation, and intangible forms of property.[593]

Bloustein insists that since Warren and Brandeis there has obviously been something unique about privacy, even if it has never been completely set out; the most significant indication of the interest is that it protects against "inviolate personality", which he

---

[589] Chris D L Hunt, "Conceptualizing Privacy and Elucidating Its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2001) 37 Queen's LJ 167 at 203−204.
[590] Immanuel Kant, *Critique of Pure Reason*, translated by Marcus Weigelt (London: Penguin Books Ltd, 2007) at 172−571; Anthony Kenny, *A New History of Western Philosophy* (Oxford: Oxford University Press, 2012) at 497–751.
[591] Edward J Bloustein, *Individual & Group Privacy* (London: Transaction Publishers, 2003) at 1−46. See the above discussion regarding Prosser *supra* note 529.
[592] Bloustein, *supra* note 591 at 4–5.
[593] *Ibid* at 5, 9–10.

interprets to be an individual's independence, dignity, and integrity.[594] He maintains that this value in privacy is a person's essence as a unique and self-determining being.[595]

Against this, it might be observed that Bloustein creates the same problems as Warren and Brandeis in terms of not adequately defining critical phrases that form the foundation of the argument to justify his point. One may ask how Bloustein comes to understand the meaning of "inviolate personality" since he commits the same blunder as Warren and Brandeis by simply deciding that the phrase means independence, dignity, integrity, and the essence as a unique and self-determining being without further elaboration to support the contention.

Yet, when discussing the difference between small-town gossip and the emergence of newspapers and other mass means of communication, Bloustein asserts that it is only with the emergence of newspapers and other mass means of communication that degradation of personality by the public disclosure of private intimacies become a legal significant reality.[596] It is only at this point that the everyday threat to personal dignity and individuality is realized.[597]

It is curious that Bloustein distinguishes between different levels of intrusion that can be involved when invading privacy—Bloustein is forward-thinking in that he is able to imagine that human dignity has the potential to be affected in different ways depending on types of technology that are used. He is able to envision that small-town gossip is not the same thing as newspapers and other mass means of communication.

Ultimately, Bloustein states that the common conceptual character of privacy that runs through all the cases he reviews involves the injury to individual freedom, personality, and dignity—in stark contrast to Prosser, Bloustein says that he can identify a single tort with a common thread.[598] In fact, he maintains that an intrusion on privacy threatens our

---

[594] *Ibid.*
[595] *Ibid.*
[596] *Ibid* at 23.
[597] *Ibid.*
[598] *Ibid* at 39.

liberty, just as an assault, battery, or imprisonment threatens our person.[599] When referring to electronic forms of eavesdropping and the electronic storage of personal data, Bloustein maintains that, while the applicable torts may differ, the social interest at issue in all cases is the preservation of individual dignity, as he so declares: "The common thread is dignity".[600]

At this point, it is helpful to understand what "dignity" actually means. It is another elusive term, which is defined as, "the state or quality of being worthy of honour or respect"; it comes from the Latin word, "*dignitās*", from "*dignus*", meaning "worthy", and "deserving".[601]

Donna Hicks states that dignity is an attribute that we are born with; plainly put, it is our inherent value and worth.[602] She distinguishes between dignity and respect; while we are all born worthy, we must earn respect.[603] She also identifies several ways in which dignity can be expressed, some of which include acknowledgment, safety, fairness, understanding, and giving others the benefit of the doubt.[604]

According to Hicks, the inevitable result of treating people with dignity is the creation of enhanced trust.[605] In fact, it is established that trust is essential for organizations to work properly, for commitment levels to remain high, and for individuals to constantly be willing to make a positive contribution.[606] What is more, trust between managers and employees is confirmed to be the primary defining characteristic of the very best workplaces.[607] She states that, when trust vanishes in the employment relationship, there are feelings of violation and betrayal that lead to a complete breakdown in the

---

[599] *Ibid*.
[600] *Ibid* at 44–46.
[601] Stenson, *supra* note 483 at *sub verbo* "dignity"; Lecturer & Morwood, *supra* note 484 at *sub verbo* "dignus".
[602] Donna Hicks, *Leading with Dignity: How to Create a Culture that Brings out the Best in People* (Michigan: Yale University Press, 2018) at 2.
[603] *Ibid.*
[604] *Ibid* at 16–17.
[605] *Ibid* at 93.
[606] *Ibid* at 93.
[607] *Ibid* at 94.

relationship.[608] In fact, with breakdowns in trust in the employment relationship, the human reaction is immediate and can lead to feelings of disgust.[609]

Ari Ezra Waldman states that trust is a social norm of interactional propriety based on favorable expectations of others' behaviour.[610] Moreover, he contends that trust is a significant factor in our decisions to share our personal information since it reduces the vulnerabilities associated with sharing.[611] He maintains that "trust is at the core of our expectations of privacy".[612]

Ultimately, Waldman argues that the relationship between privacy and trust is functional, in that privacy builds trust, and trust yields disclosure.[613] In fact, he asserts that if we want privacy to thrive in a world that requires significant disclosures to participate in modern life, we need sharing in some contexts to be compatible with privacy.[614] When doing so, it is important to recognize that many disclosures are not purely voluntary, and privacy that factors in trust can rebalance power relationships; for example, the power dynamics of doctor-patient relationships are situations where disclosure is necessary, but the trust norms that have been developed over time through ethics and duties of loyalty operate to soften the disclosure risks so the information holders are less vulnerable.[615]

In the workplace, trust allows individuals to deal with uncertainty and complexity, take risks, cooperate with others, and create order in chaos, because the norms we expect others to follow, namely confidentiality and discretion, are essential for creating circumstances for sharing information.[616] Consequently, the existence of trust in work relationships can lead to outperformance of competitors, increased efficiency of teamwork and cooperation, and an increase in the level of dedication to a company

---

[608] *Ibid* at 95.
[609] *Ibid* at 95−96
[610] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018) at 50.
[611] *Ibid.*
[612] *Ibid.*
[613] *Ibid* at 61.
[614] *Ibid.*
[615] *Ibid* at 61–62, 73.
[616] *Ibid* at 74.

mission; most importantly, trust helps individuals connect and share more meaningful interactions.[617] Privacy provides benefits to both individuals and corporations because privacy is bound to trust, and this is a fundamental requirement in life.[618]

George Kateb states that, while human dignity is perceived to be the basis for human rights, not many understand what dignity is and why it matters for the claim to rights.[619] He argues that the idea of human dignity is something that is necessary to the theory of human rights; he insists that human dignity must be affirmed.[620] In fact, he explains that, "the idea of human dignity not only serves to help defend the theory of individual rights but also gives a perspective on the dignity of the human species".[621] He begins with the assumption that the dignity of every human being has a status that is equal to that of all others.[622] Consequently, equal status means that no one person is better than another, despite the fact that individual talents and innate abilities may vary.[623] In particular, such variations in humans are irrelevant to human status.[624]

Alexandra Rengel draws on natural law and applies the dignity/human rights approach to the concept of privacy, asserting: "Privacy is an essential human need".[625] According to Rengel, humans need to know that they can keep some things secret from others, and the right to have secrets is so embedded in human nature that it would be very difficult to imagine satisfying human interactions without the ability to keep certain things secret from each other and to lead lives unmonitored by others.[626]

Rengel argues that the need for humans to have a certain degree of privacy is natural, and due to this intrinsic need, privacy is recognized in a social and legal sense in most

---

[617] *Ibid*.
[618] *Ibid* at 75.
[619] George Kateb, *Human Dignity* (Cambridge: Harvard University Press, 2011) at 1.
[620] *Ibid* at 5.
[621] *Ibid*.
[622] *Ibid* at 5–9.
[623] *Ibid* at 9.
[624] *Ibid*.
[625] Alexandra Rengel, *Privacy in the 21st Century* (Netherlands: Koninklijke Brill, 2013) at 1.
[626] *Ibid*.

cultures.[627] She stresses the importance of acknowledging the intrinsic and natural quality of the human need to privacy.

Lastly, James Griffin provides further clarification on the underlying reasons for the existence of human rights.[628] Griffin describes human rights as rights we have simply by virtue of being human.[629] He suggests that the Latin word, "*ius*" is a "right" that an individual has and that derives from the natural law that all human beings are, in a very particular sense, equal.[630] What is more, the link between freedom and dignity has been carried through to the present.[631] Griffin maintains that human rights are currently seen as protections of our normative agency, or personhood.[632] However, Griffin states this is not exactly clear where the line should be drawn; he proposes that to answer this question, it is necessary to consider whether the right is too complicated to achieve its goal, or too demanding, and also how human beings in societies actually work and consider the practicalities.[633]

Griffin suggests that it is possible to make a case for a human right of privacy, because without privacy, autonomy would be threatened.[634] According to Griffin, we are social animals and we seek acceptance by the group; in fact, it is rare to swim against strong social currents.[635] He contends that if our deliberation decisions about how we live were open to public scrutiny, we would self-censor and act in self-defence.[636] Griffin states that autonomy is a feature of deliberation and decision, and liberty is a feature of action concerned with pursuing one's aims without interference.[637]

Notwithstanding this helpful clarification of human rights, Griffin subsequently states that, while informational privacy is not the ideal name given that it is too narrow, current

---

[627] *Ibid*.
[628] James Griffin, "The Human Right to Privacy" (2007) 44 San Diego L Rev 697.
[629] *Ibid* at 697.
[630] *Ibid*.
[631] *Ibid* at 698–699.
[632] *Ibid*.
[633] *Ibid* at 699–700.
[634] *Ibid* at 700.
[635] *Ibid*.
[636] *Ibid*.
[637] *Ibid*.

appeals to the human right of privacy are too broad.[638] He takes a peculiar turn and proceeds to argue that human rights can be reduced to two rights when privacy claims are involved: the right to informational privacy, and the right to liberty.[639] This strategy attempts to negate the approach initially taken, namely drawing on an understanding of human rights in order to argue for a right to privacy.

One may challenge this proposal and refer to it as another case of déjà vu, where a theorist attempts to divide the concept of privacy into a certain number of rights that are to be protected in the courts. This fragmentation of the concept of privacy is just another example of what takes place in Prosser's analysis. One may introduce another challenge: Griffin writes from the privacy perspective of dignity/human rights, but then highlights the necessity of considering whether the right is too complicated to achieve its goal and too demanding; he questions how human beings in societies actually work and considers the practicalities. Griffin appears to be struggling with how to apply this theory in a practical manner, and his solution is to divide privacy into informational privacy and liberty.

Perhaps this is because the theory of dignity/human rights appears to run into roadblocks when realistically converting broad, vague, utopian ideas of what "should" be into what can be done realistically. Indeed, this is one of the main criticisms of the theory—the concept of dignity is too broad to be practical and lacks detail, and this prevents any kind of meaningful application. Another roadblock is that the theory uses complex terms such as personality and liberty without providing any solid explanation. Certain terms are also conflated with dignity, including autonomy and personality. Another roadblock that weakens the theory is that some of these terms pertain to competing interests, and the theory does not explain how competing interests can be balanced or dealt with in any way.

While at first glance there is concern about realistic application of this theory, it is important to remember that the use of ambiguity in the language of human rights enables

---

[638] *Ibid* at 702–703.
[639] *Ibid* at 717.

a more organic and flexible approach for understanding privacy, adapting to the evolving society, and balancing competing interests.[640] Given that privacy is fundamental and something to which individuals are equally entitled by virtue of their status as persons, it is critical to keep in mind that this approach enables a liberal and purposive interpretation where privacy rights receive a broad interpretation and exceptions are narrowly construed.[641] As a starting point, the dignity/human rights approach appreciates the inherent value and worth of all individuals.

Practically speaking, if the dignity/human rights perspective is to be the prevailing approach in Canada, then it would follow that a core societal value is that privacy is to be treated as an end, and Canadians deserve to be treated with dignity in a way that respects self-determination, autonomy, self-respect, and personality. It would also follow that the privacy of Canadians is to be regarded as fundamental and not something that can be taken away, given up, or used as a means to manipulate or gain value. Accordingly, using this theory, individuals (and their personal information) would therefore need to be respected so that their innate worthiness is maintained.

3.3 Conclusion

As can be seen from the above analysis, even when using a neutral investigation of privacy as a starting point, most theories of privacy are non-reductionist. By this I mean that they appreciate that there is a coherent value to privacy, that there is something that is inherently unique and valuable that cannot be covered off by some other law or set of laws. All the same, many non-reductionist theories fall short of sufficiently answering the question, "What is privacy, and why is it important?" Many of the theories, when combined, could create a more complete picture of what privacy involves, but if this is what is required in order to disentangle the concept of privacy, than these theories are neither sufficient nor necessary answers to the question.

This Chapter explored the strengths and weaknesses of selected theories of privacy.

---

[640] Ruth Sullivan, *Sullivan on the Construction of Statutes*, 5th ed (Markham, Ontario: LexisNexis Canada Inc, 2008) at 255−297, 497−507.
[641] *Ibid*.

The reductionist theories are the most problematic as they are lacking in depth. The cluster-of-rights perspective adopted by, for example, Thomson, is unconvincing. The analysis is shallow, overly skeptical, and short-sighted. Posner's economic theory of privacy treats information as a commodity and does not acknowledge that some may not appreciate what is being sacrificed in an exchange until it is too late. In this cold and mechanical analysis, the main motivation of privacy is to hide information, manipulate others, or gain something in exchange for value and efficiency. It leaves minority groups and vulnerable citizens behind.

Many of the non-reductionist theories are also problematic, but for different reasons. Approaches that adopt the idea that invasion of privacy is a tort uses undefined terms, operates from a dystopian view of technology, and links privacy to morality and justice without explaining why it is a good idea to do this. This viewpoint comes across as declaratory rather than analytical. Some advocates for the tort attempt to partition the concept of privacy into separate rights without providing enough explanation to justify the action. This also results in the concept of privacy becoming nothing separate in itself that is worth protecting.

Although the feminist theories may shed light on the interests of vulnerable citizens, they do not provide any real solutions to the problems that they identify, while the control-over-information perspective fails to identify the types of information that are within a person's control and is consequently too vague. Certain words such as "control" and "personal information" are left undefined. The problem is that even if one adopts this perspective it is unclear how this theory differs from the economic theory, since a person can decide when to allow someone to become aware of certain information within a person's control—typically when a person wants something in exchange. Also, there are no clear limits especially in the case of sensitive persons.

While the pragmatic, contextual approach offers a realistic, flexible, and open understanding of privacy that is aligned to the reasonable expectations of an evolving society, in my view it is too complex and has the effect of diluting the meaning of privacy. Though it is more realistic than most, with its modern inclination and attempt to

grasp the complexities of the technological context, the theory's unintended consequences are simply too high a price for society to pay. There needs to be something representing core societal values that can undergird all analyses.

The dignity/human rights approach, the dominant approach that I use during this dissertation, provides a more helpful understanding of privacy that enables the use of language to broadly and liberally interpret the law. The approach allows for a purposive interpretation and helps decision makers make incremental modifications to adapt with an evolving society and also to achieve appropriate balances when assessing competing interests.

Since the dignity/human rights theoretical perspective of privacy is the lens that I use when understanding privacy and constructing a new workplace privacy regime, I spent a considerable amount of time discussing the nature of dignity, trust, and how individuals are inherently worthy and deserving of privacy. This ultimately affects how I approach the task of interpreting the upcoming privacy provisions and workplace privacy cases, and building the new workplace privacy regime.

Recognizing privacy as a fundamental right, the dignity/human rights perspective emphasizes viewing and treating individuals and their privacy as ends rather than means. Privacy is not something to use in order to get something. Privacy is not something to utilize in order to create value. The message is simple. Privacy is always valuable—for everyone.

Chapter 4

4 Analysis: Examination of Privacy Provisions

As mentioned in the Introduction, the purpose of this Chapter is to analyze various privacy provisions from Canada, the United States, and the European Union.

The Canadian privacy provisions are from: *Québec Charter*;[642] *PIPEDA*[643] (including the *PIPEDA Breach Regulations*[644]); *BC PIPA*;[645] and the *QC Act*.[646] There is also a discussion of Canada's *Bill S-21(Privacy Rights Charter)*.[647] The privacy provisions from the United States have been chosen from: *California Constitution*;[648] *California Consumer Privacy Act*;[649] *California Labor Code*,[650] and the *California Civil Code (Customer Records)*.[651] There is also an examination of privacy provisions in these American bills: *Bill S5642 (New York Privacy Act);*[652]and *Bill SB 6280 (Washington Facial Recognition)*.[653] The privacy provisions from the European Union come from: *EU Convention*;[654] and the *GDPR*.[655]

---

[642] *Charter of Human Rights and Freedoms*, CQLR c C-12 [*Québec Charter*].
[643] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
[644] *Breach of Security Safeguards Regulations* (SOR/2018-64) [*PIPEDA Breach Regulations*].
[645] *Personal Information Protection Act*, SBC 2003, c 63 [*BC PIPA*].
[646] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 [*QC Act*].
[647] Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess, 37th Parl, 2001 (first reading 13 March 2001, dropped from the Senate Order Paper in 2002) [*Bill S-21 (Privacy Rights Charter)*].
[648] Cal Const art I [*California Constitution*].
[649] *California Consumer Privacy Act of 2018*, 3 CIV 1.81.5 (2018) [*California Consumer Privacy Act*].
[650] Cal Lab Code (2012) [*California Labor Code*].
[651] Cal Civ Code, 3 CIV 1.81 (2000) [*California Civil Code (Customer Records)*].
[652] US, SB 5642, *New York Privacy Act*, 2019−2020, Reg Sess, NY, 2019 [*Bill S5642* (*New York Privacy Act)*]. Bill S5642 was introduced into the Senate, read twice on May 9, 2019 and January 8, 2020, and referred to the Committee on Consumer Protection on those dates. See New York State Senate, "Senate Bill S5642" (2020) online: *New York State Senate* <https://www.nysenate.gov/legislation/bills/2019/s5642>.
[653] US, SB 6280, *Concerning the Use of Facial Recognition Services*, 2019−2020, Reg Sess, Wash, 2020 (passed by the Senate and the House on March 12, 2020 and signed by the Governor but with a partial veto on March 31, 2020; sections 1 to 9 and sections 11 to 13 become effective July 1, 2021 and will form part of RCW, Title 43, Chapter 257) [*SB 6280 (Washington Facial Recognition)*]. See also Washington State Legislature, "Bill Information: SB 6280" (12 April 2020), online: *Washington State Legislature* <https://app.leg.wa.gov/billsummary?BillNumber=6280&Initiative=false&Year=2019>.
[654] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5 (1950) [*EU Convention*].
[655] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of*

Although it may be tempting to import entire bills, statutes, regulations, or conventions from what appear to be stronger, privacy-protective jurisdictions, this kind of transplantation from one jurisdiction to another is not recommended by comparative legal methodologists, because when rules of one jurisdiction cross boundaries, they may undergo a transformation to the point where their meaning can become displaced.[656] Rather, it is important to respect the cultural contexts of the jurisdictions examined and find more effective ways of borrowing ideas and fitting them into the Canadian jurisdiction following a careful analysis of similarities and differences between the provisions of the jurisdictions, for the purpose of finding practical solutions to similar problems in areas with different legal systems.[657]

In line with this reasoning, Elizabeth Denham,[658] the United Kingdom Information Commissioner and former Information and Privacy Commissioner for British Columbia, has recognized the benefits of the most recent European Union privacy instrument, the *GDPR*, and has remarked during a podcast by Michael Geist:

> I'm not advocating for the details and prescription of the *GDPR* to be translated into Canadian law, but I think some of the rights and some of the powers for regulators need to find an even playing field, a harmonized approach.[659]

---

such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L119/1 [*GDPR*].

[656] Geoffrey Samuel, "Comparative Law and its Methodology" in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 121 at 124–134, online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315386669>; Mark Van Hoecke, "Methodology of Comparative Legal Research", Law and Method (December 2015) 1 at 3−6, 11, 28, 30, online: *Law and Method* <http://www.lawandmethod> DOI: <10.5553/REM/.000010>; Mathias M Siems, "The Curious Case of Overfitting Legal Transplants" in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 133 at 136−138.

[657] *Ibid*.

[658] Elizabeth Denham is currently (as of April, 2020) the UK Information Commissioner at the Information Commissioner's Office in Cheshire. She is the former Information and Privacy Commissioner for British Columbia, and also the former Assistant Privacy Commissioner of Canada. See Information Commissioner's Office, "Elizabeth Denham CBE, Information Commissioner" (2020), online: *Information Commissioner's Office* <https://ico.org.uk/about-the-ico/who-we-are/information-commissioner/>.

[659] Michael Geist, "The LawBytes Podcast, Episode 2: "It's Time to Modernize the Laws"" (11 March 2019) at 17m:37s−17m:56s, online (podcast): *Michael Geist* <http://www.michaelgeist.ca/2019/03/the-lawbytes-podcast-episode-2-its-time-to-modernize-the-laws/>.

Thus, in the interests of harmonization of law,[660] it is advantageous to investigate several types of strong privacy provisions from the selected jurisdictions and determine whether it is possible to borrow ideas from them in order to close the electronic surveillance gap in the Canadian context.

A useful approach for maintaining the focus of this dissertation is to compare a small number of privacy provisions that concern common topics. A mix of selected privacy provisions of the various jurisdictions are discussed under three themes: (1) foundational principles touching on privacy and electronic surveillance;[661] (2) consent and balancing rights with legitimate interests;[662] and (3) order-making powers, penalties, and fines.[663]

As mentioned in the Introduction, the privacy provisions fall under the three features of privacy provisions, which represent areas of law relevant to privacy: (1) constitutional and human rights provisions; (2) data protection provisions; and (3) employment provisions. Aspects of each of the features of privacy provisions are discussed within the three themes as they become relevant. Each of these features must be examined in order to form a complete understanding of privacy and electronic surveillance.

I have chosen these themes because they encapsulate several interesting issues relating to the electronic surveillance gap in employment. Theme 1 investigates foundational principles for understanding privacy and electronic surveillance: data collection and processing; profiling and unreasonable electronic surveillance; fair information principles; legislative purposes; privacy by design; data impact risk assessments; rights-

---

[660] Van Hoecke, *supra* note 656 at 2.
[661] The following provisions will be discussed for theme (1): *PIPEDA*, s 3, Schedule 1, cl 4.2, 4.4; *Québec Charter*, s 5; *Bill S-21 (Privacy Rights Charter)*, ss 1−5; *California Consumer Privacy Act*, § 1798.140; *Bill S5642 (New York Privacy Act)*, § 1102; *Bill SB 6280 (Washington Facial Recognition)*, §§ 1, 2, 3, 8, 11; *California Constitution*, art 1, § 1; *GDPR*, arts 1, 4, 5, 9, 21, 22, 23, 25, 35; *EU Convention*, art 8. See Appendix A.
[662] The following provisions will be discussed for theme (2): *PIPEDA*, ss 2(1), 6.1, 7(1)−7(3), 7.1–7.4 10.1–10.3, Schedule 1, cl 4.3; *PIPEDA Breach Regulations*, ss 2–6; *QC Act*, s 14; *BC PIPA*, ss 7−9, 13, 16, 19; *California Consumer Privacy Act*, §§ 1798.120, 1798.125, 1798.145; *California Labor Code*, § 980; *California Civil Code (Customer Records)*, §§1798.81.5, 1798.82; *GDPR*, arts 4, 6−7, 33−34, 88. See Appendix B.
[663] The following provisions will be discussed for theme (3): *PIPEDA*, ss 14–16, 17.1–17.2, 28; *BC PIPA*, ss 52–53, 56–57; *QC Act*, ss 55, 58, 91–93; *California Consumer Privacy Act*, §1798.155; *GDPR*, arts 58, 83–84. See Appendix C.

based data protection provisions; and data fiduciaries. Theme 2 explores: definitions of consent; employees' ability to provide, withhold, and revoke consent in situations involving electronic surveillance; and strategies for facilitating an effective balance of employees' privacy interests and employers' legitimate business interests. Theme 3 considers the creation and enforcement of meaningful orders, penalties, and fines to strengthen the privacy regime. As can be seen from the chart below, a mix of core privacy provisions are examined in each theme.

Table 1: Jurisdictions and Themes of Privacy Provisions in Chapter 4

Themes	Canada	United States	European Union
1- Foundational principles touching on privacy and electronic surveillance	*PIPEDA* *Québec Charter* *Bill S-21 (Privacy Rights Charter)*	*California Consumer Privacy Act* *Bill S5642 (New York Privacy Act)* *Bill SB 6280 (Washington Facial Recognition)* *California Constitution*	*GDPR* *EU Convention*
2- The consent of individuals and the legitimate interests of organizations	*PIPEDA* *PIPEDA Breach Regulations* *BC PIPA* *QC Act*	*California Consumer Privacy Act* *California Labor Code* *California Civil Code (Customer Records)*	*GDPR*
3- Order-making powers, penalties, and fines	*PIPEDA* *BC PIPA* *QC Act*	*California Consumer Privacy Act*	*GDPR*

I examine several Canadian privacy provisions in order to understand what currently exists in Canada and to identify any gaps that need filling with respect to electronic surveillance in the employment context.[664] I examine privacy provisions in the United States and the European Union in order to understand how the privacy provisions are crafted, especially in situations where concepts in the theme are not covered in the Canadian privacy regime at all.[665] The provisions that I have picked are relatively stronger privacy provisions so that I can glean as much information as possible from the analyses and ultimately strengthen protections in Canada.

This dissertation asks how the principles and values that emerge from selected privacy provisions can be used to close the electronic surveillance gap in employment using a design that fits into Canada's legal system. By "principles", I mean fundamental truths or propositions that serve as the foundation for a system of belief, behaviour, or chain of reasoning; it is the fundamental source of something.[666] By "values", I mean the regard that something is held to deserve, and the importance, worth, or usefulness of something; it includes the standards of behaviour that are judged to be important in life.[667]

When conducting my analysis, I will pay particular attention to the language and the structure of the provisions to isolate useful elements that can be used when crafting the proposed workplace privacy regime. Since the priority is on identifying and filling gaps in Canada's regime, it is advantageous to compare similar provisions side-by-side and note subtle differences for the purposes of construction. Further, it is useful for the comparison to go beyond the level of legislation, and aim to understand the social reality involved.[668] To that end, this Chapter contains a thorough analysis of privacy provisions,

---

[664] Note that provisions in Alberta's *AB PIPA* are very similar to those in British Columbia's *BC PIPA*, so I settled on examining only the *BC PIPA*. See *Personal Information Protection Act*, SA 2003, c P-6.5 [*AB PIPA*].
[665] Note that provisions in a recent American federal bill, *Bill S 3744 (Data Care Act)*, are very similar to those in *Bill S5642 (New York Privacy Act)*, so I settled on examining only *Bill S5642 (New York Privacy Act)*. See US, Bill S 3744, *Data Care Act of 2018*, 115th Cong, 2018 [*Bill S 3744 (Data Care Act)*].
[666] Angus Stenson, ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010) *sub verbo* "principle".
[667] *Ibid* at *sub verbo* "value".
[668] Van Hoecke, *supra* note 656 at 7; Darren O'Donovan, "Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls" in Laura Cahillane & Jennifer Schweppe, eds, *Legal*

and ties into the discussion various relevant social theory ideas involving surveillance and privacy.

As will be seen below, this Chapter suggests that there are currently insufficient legislative privacy protections in Canada's legal regime compared to other jurisdictions for closing the electronic surveillance gap in employment. Moreover, it will show that principles and values can be extracted from the privacy provisions, and can be used to design a new workplace privacy regime that sufficiently closes the electronic surveillance gap in a way that fits into Canada's current legal system.

This Chapter is organized by theme. It begins with broad concepts, and gradually becomes more focused on specific issues. In this Chapter, I examine each theme for the purposes of achieving three goals. First, I note the provisions that fall within each theme. Second, I analyze the provisions of each theme, discuss the principles and values that emerge from the analysis, and discuss how the identified gaps in Canada's regime can be filled through the exploration of privacy provisions of the studied jurisdictions. And third, I set out my ideas for incorporating the detected principles and values into the proposed workplace privacy regime to close the electronic surveillance gap. These ideas stem from my discussion of the implications for the new workplace privacy regime. At this stage, the ideas are not yet crafted into detailed provisions. In Chapter 6, I will discuss how I propose to fit my ideas into the framework of Canada's legal system.

4.1 Theme 1: Foundational Principles Touching on Privacy and Electronic Surveillance

The first theme discusses selected provisions involving foundational principles for understanding privacy and electronic surveillance. I list the provisions in the theme, analyze the provisions, and discuss the implications for the new workplace privacy regime.

Research Methods: Principles and Practicalities (Dublin: Clarus Press Ltd, 2016) 107 at 108, 116; Fiona Cownie & Anthony Bradney, "Socio-Legal Studies" in Watkins & Burton, *supra* note 656, 40 at 42−46.

4.1.1 The Privacy Provisions Examined in Theme 1

As can be seen in the chart below, there are two features of privacy provisions, namely data protection provisions, and constitutional and human rights provisions, which will be examined in Theme 1:

Table 2: The Privacy Provisions Studied in Chapter 4, Theme 1

Theme	Canada	United States	European Union
1- Foundational principles touching on privacy and electronic surveillance	*PIPEDA* *Québec Charter* *Bill S-21(Privacy Rights Charter)*	*California Consumer Privacy Act* *Bill S5642 (New York Privacy Act)* *Bill SB 6280 (Washington Facial Recognition)* *California Constitution*	*GDPR* *EU Convention*

4.1.2 Analysis of the Privacy Provisions in Theme 1

My goal in this section is to argue that *PIPEDA* contains significant gaps and does not sufficiently address issues related to electronic surveillance; additionally, there are ways to fill those gaps by examining how other jurisdictions have legislatively tackled the issues.

I will argue for this conclusion in three steps. First, I will discuss problematic definitions and conceptualizations regarding certain terms in *PIPEDA*. Second, I will show that there are challenges with provisions in Schedule 1 of *PIPEDA*[669] regarding electronic surveillance in employment, and it is necessary to create new provisions to deal with them. Third, I will explain that, given these gaps in *PIPEDA*, it is necessary to examine

[669] *PIPEDA*, *supra* note 643 at Schedule 1.

the strategies used by other jurisdictions to enhance trust in the new workplace privacy regime.

To that end, the first thing to mention is that Canada's *PIPEDA* does not define "collection", "processing", "automated", "monitoring", or "electronic surveillance".[670] The most helpful guidance in this regard is found in the guidelines created by the Office of the Privacy Commissioner of Canada when dealing with monitoring of employees' social media,[671] and also covert video surveillance in the private sector.[672] In both cases, the same conclusion is reached: tracking employees' personal-based or work-based social media and the capturing of images of identifiable individuals through covert video surveillance are both considered to be a "collection" of personal information.[673] In sum, *PIPEDA* does not provide clear definitions of what I consider to be important and distinct concepts, as I will explain below.[674]

In contrast, California explicitly defines both collection and processing in its *California Consumer Privacy Act.*[675] There "collection" is broadly described as buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means; it includes receiving information from the consumer, either actively or passively, or by observing the consumer's behaviour.[676] "Processing" is

---

[670] *Ibid* at s 2.
[671] Office of the Privacy Commissioner of Canada, "Privacy and Social Media in the Workplace" (August 2019), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_41_sn/> [Privacy Commissioner, "Social Media"].
[672] Office of the Privacy Commissioner of Canada, "Guidance on Covert Video Surveillance in the Private Sector" (May 2009), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/> [Privacy Commissioner, "Video Surveillance"]. Although the Office of the Privacy Commissioner of Canada created guidelines regarding overt video surveillance in the private sector in March 2008, these guidelines have to do with overt video surveillance of the public by private sector organizations in publicly accessible areas such as inside stores or outside buildings, and do not apply to the surveillance of employees. See Office of the Privacy Commissioner of Canada, "Guidance on Overt Video Surveillance in the Private Sector" (March 2008), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gl_vs_080306/>.
[673] Privacy Commissioner, "Social Media", *supra* note 671; Privacy Commissioner, "Video Surveillance", *supra* note 672.
[674] *PIPEDA*, *supra* note 643 at s 2.
[675] *California Consumer Privacy Act*, *supra* note 649 at § 1798.140(e), (q).
[676] *Ibid* at § 1798.140(e).

broadly defined and means "any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means; it does not provide a list of actions that pertain to processing".[677]

Article 4(2) of the European Union's *GDPR*,[678] broadly defines the single term of "processing" as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; it provides an extensive list of actions that involve processing, including collection, use, and disclosure.

When placing these definitions side-by-side, it is clear that *PIPEDA* provides the least amount of legislative direction compared to the provisions in the *California Consumer Privacy Act*[679] and the *GDPR*.[680] Relatively speaking, in other words, Canada is in the worst position compared to California and the European Union. Canada needs to explicate in *PIPEDA* what is meant by "collection" and "processing", either by providing definitions of both collection and processing, or a single wider definition of processing that encapsulates both concepts. Either way, there must be a definition of processing by automated means.

To be sure, I am not suggesting that processing by automated means and electronic surveillance can be understood to be exactly the same; on the contrary, I believe they are distinct concepts, and I use them as such throughout this dissertation. Automated processing, a subset of processing, involves electronic or automatic processing to perform most tasks.[681] Although electronic surveillance may be a subset of automated processing, it is important to discern the unique features of electronic surveillance because they

---

[677] *Ibid* at § 1798.140(q).
[678] *GDPR*, *supra* note 655 at art 4(2).
[679] *California Consumer Privacy Act*, *supra* note 649 at § 1798.140(e), (q).
[680] *GDPR*, *supra* note 655 at art 4(2).
[681] Ian Brookes et al, eds, *Collins English Dictionary*, 13th ed (Glasgow: HarperCollins Publishers, 2018) *sub verbo* "automated".

involve active targeted monitoring of one or more persons, synonymous with monitoring or tracking; this distinct and exclusive concept of "electronic surveillance" has been considered to be "the systematic creation and/or use of personal data for the investigation or monitoring of actions or communications of one or more persons".[682] The idea of monitoring is incorporated in this definition of electronic surveillance; indeed, "to monitor" is defined as "observe or check the progress or quality of something over a period of time", "keep under systemic review", and "maintain regular surveillance over".[683] The point made in this part is that there are no definitions in *PIPEDA* regarding any of these terms involving collection, processing, automated, monitoring, or electronic surveillance; in my view, it is useful to examine how other jurisdictions have approached the issue legislatively so that some of the ideas can be included in *PIPEDA*. I would like to suggest that there be an addition of "processing", which would include "collection", and also an addition of "electronic surveillance" as described above as having an unparalleled focus on the targeted monitoring of individuals.

Not only is there an absence of essential definitions relating to electronic surveillance in *PIPEDA*, but there are also no specific provisions that expressly address data privacy concerns that arise as a result of electronic surveillance.[684] This makes Canada unresponsive to rapidly changing electronic surveillance technologies, and insensitive to the needs of Canadians who require sufficient protections.

There are serious threats associated with electronic surveillance, since automated data collection and processing go even further than what Foucault imagined with the monitoring gaze, internalization, and self-censorship of subjects in his circular cage, the

---

[682] Roger Clarke & Graham Greenleaf, "Dataveillance Regulation: A Research Framework" (2017) 25:1 J L Info & Sci 104 at 105, 108.
[683] Stenson, *supra* note 666 at *sub verbo* "monitor".
[684] As mentioned above, it is acknowledged that the Office of the Privacy Commissioner of Canada has released a couple of brief documents providing guidance on surveillance issues in the private sector; however, I argue that this is insufficient to tackle the issue, and insist that explicit legislative provisions are required in order to adequately deal with current concerns regarding electronic surveillance and closing the electronic surveillance gap. See *supra* notes 671−672.

Panopticon;[685] in particular, "always-on" monitoring can facilitate predictions using automation.[686] Most strikingly, electronic surveillance creates a potential for exploitation of individuals and an abuse of surveillance power.[687] One hazardous aspect of this phenomenon is that of function creep, or the repurposing of personal information for new uses, where the new purposes are created without the knowledge of data subjects.[688]

That is, when we engage in online activity, the opportunities for monitoring escalate as we participate in our own surveillance, captured by all entities including governments, employers, and businesses; what is most disturbing is that these entities use the information generated by ubiquitous surveillance efforts for their own purposes.[689] For instance, we as a society like to stay connected with people online, posting content, tagging photos, and liking pictures or videos.[690] The danger is that electronic surveillance is primarily conducted by capital to control behaviour and exploit surplus value generated by users.[691] The alarming result is that large tech companies extract data, exploit users through monitoring efforts, and create profiles to assess behavioural data to determine what individuals are thinking and feeling at any moment.[692] Even though this extracted

---

[685] Michel Foucault, *Power/Knowledge: Selected Interviews & Other Writings 1972–1977*, edited by Colin Gordon, translated by Colin Gordon et al (New York: Vintage Books, 1980) at 147, 208 [Michel Foucault, "Power/Knowledge"].
[686] Mark Andrejevic, "Automating Surveillance" (2019) 17:1/2 Surveillance & Society 7 at 7–10 online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> [Mark Andrejevic, "Automating Surveillance"].
[687] *Ibid* at 7.
[688] Mark Andrejevic, "Surveillance in the Big Data Era" in Kenneth D Pimple, ed, Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards (New York: Springer, 2014) 55 at 67–68 [Mark Andrejevic, "Big Data Era"].
[689] Colin J Bennett et al, *Transparent Lives: Surveillance in Canada* (Edmonton: AU Press, Athabasca University, 2014) at ix, 168, 170 –171, 179 [Bennett et al, "Transparent Lives"].
[690] *Ibid* at 167–170.
[691] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) at 276–277 [Christian Fuchs, "Web 2.0"]; Christian Fuchs, "Political Economy and Surveillance Theory" (2012) 39:5 Crit Sociology 671 at 685, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1177/0896920511435710> [Christian Fuchs, "Political Economy"]; Nicole S Cohen, "The Valorization of Surveillance: Towards a Political Economy of Facebook" in Monahan & Wood, *supra* note 691, 298 at 298.
[692] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30 Journal of Information Technology 75 at 78–82, online (pdf): SAGE Journals <journals.sagepub.com> DOI: <10.1057/jit.2015.5> [Shoshana Zuboff, "Big Other"]; Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019) at 69–70, 227, 275, 293–296 [Shoshana Zuboff, "Surveillance Capitalism"].

data may be taken from outside the workplace, it can be used in concerning ways that affect all aspects of life, including employment.[693] Indeed, the combination of increasingly frequent social media and digital device use alone has led to a troubling situation where we as a society are becoming hard-wired for electronic surveillance—and digital devices can easily become tools that are used for oppressive purposes.[694] What is more, through the use of learning theories, the ultimate goal of technology companies is to predict behaviours and modify real-time actions using various manipulation strategies to the point where inevitabilism may ensue and individuals believe that they have been stripped of their free will.[695]

And still, there remains a privacy paradox.[696] The paradox is this: even though we know about the dangerous potential of the abuse of power by larger technology companies, we still give up our personal information freely and fully, and voluntarily participate in the surveillance culture.[697] The result is that we end up voluntarily rendering ourselves virtually transparent to anyone, thereby making it easier to monitor us, target us, track us, and even punish us.[698] We even expose ourselves to potential discrimination based on panoptic sorting, where people are sorted according to their presumed economic or political value and may become subject to discrimination based on these groupings, including racial profiling.[699]

Not only are employees exposed outside the workplace through ubiquitous surveillance, but they are also unveiled inside the workplace; electronic surveillance during working

---

[693] Bennett et al, "Transparent Lives", *supra* note 689 at 168, 179.
[694] *Ibid* at 36.
[695] Shoshana Zuboff, "Big Other", supra note 692 at 78–82; Shoshana Zuboff, "Surveillance Capitalism", *supra* note 692 at 69–70, 227, 275, 293–296.
[696] David Lyon, *The Culture of Surveillance* (Cambridge: Polity Press, 2018) at 115–117 [David Lyon, "Culture of Surveillance"]; Alyson Leigh Young & Anabel Quan-Haase, "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited" (2013) 16:4 Information, Communication & Society 479 at 479−481, online (pdf): *Taylor & Francis* <www-tandfonline-com> DOI: 10.1080/1369118X.2013.777757 [Young & Quan-Haase, "Privacy Protections"].
[697] *Ibid*.
[698] Bernard E Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015) at 13–14.
[699] Oscar H Jr, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, Co: Westview Press, 1993) at 1–2 [Gandy, Jr, "The Panoptic Sort"]; Oscar H Gandy, Jr, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage* (Surrey: Ashgate, 2009) at 124 [Gandy, Jr, "Chance"].

hours creates a certain visibility through the use of panoptic power, whereby information systems can translate, record, and display human behaviour with high degrees of illumination.[700] The result of this unsettling transparency is that employees feel vulnerable, untrusting, powerless, and filled with despair at the thought of losing self-control, unique identities, and autonomy.[701]

This is why Canadian citizens, who all have inherent value and worth,[702] are in need of protection from acts of unreasonable electronic surveillance in the form of strong data protections provisions. Trust is at the core of our expectations of privacy and is a significant factor in our decisions to share our personal information, since it reduces the vulnerabilities related to sharing.[703] Affording individuals with protections helps to build trust, which then leads to further comfort with the notion of disclosing personal information.[704] Moreover, these protections have the potential to rebalance power relationships since they soften the disclosure risks and cause individuals to become less vulnerable.[705] This makes a difference in the workplace, since trust bolsters human connections and can lead to outperformance of competitors, increased efficiency of teamwork and cooperation, and an increase in the level of dedication to a company mission.[706] In fact, the inevitable result of treating people with dignity is the creation of enhanced trust, and trust is essential for organizations to work properly.[707] This is demonstrated when individuals rate higher on workplace performance measures and are more willing to work together to help each other and the company as well.[708]

While *PIPEDA* is silent on the issue of electronic surveillance, it is important to note that other jurisdictions have made considerable progress in providing necessary protections,

---

[700] Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York: Basic Books, 1988) at 322–327 [Shoshana Zuboff, "Smart Machine"].
[701] *Ibid* at 344, 404.
[702] Donna Hicks, *Leading with Dignity: How to Create a Culture that Brings out the Best in People* (Michigan: Yale University Press, 2018) at 2.
[703] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018) at 50.
[704] *Ibid* at 61.
[705] *Ibid* at 61–62, 73.
[706] *Ibid* at 74.
[707] Hicks, *supra* note 702 at 93–99.
[708] *Ibid*.

and have created provisions that are particularly instructive when it comes to understanding the sorts of features that are essential in a legislative framework to tackle issues regarding electronic surveillance.

As mentioned above, "processing" in Article 4(2) of the *GDPR*[709] is broadly defined and includes a wide array of operations that can be performed on personal data, automated or not. What is most relevant to this discussion is the definition of "profiling" in Article 4(4) of the *GDPR*,[710] which involves any form of automated processing of personal data that has a goal of using personal data to analyze, evaluate, and predict aspects relating to a natural person. Article 9(1) of the *GDPR*[711] prohibits the processing of personal data regarding special categories of personal data such as a person's racial or ethnic origin.[712] In fact, Article 21(1) of the *GDPR*[713] provides individuals with the right to object to the processing of personal data, including profiling.[714] Article 22 of the *GDPR*[715] goes even further and discusses automated individual decision-making including profiling, and it provides individuals with the right not to be subject to a decision based solely on automated processing, including profiling. These rights are balanced with legitimate interests set out in Article 23 of the *GDPR*[716] so there is a fair consideration of competing interests, such as defence or national security. Still, when there is a restriction, there are specific requirements that must be met.[717]

The panoptic sort has been considered a system of social control where more vulnerable individuals, including groups whose information could be subject to the automated processing referred to in Articles 4(4) and 9(1) of the *GDPR*[718] are organized based on

---

[709] *GDPR, supra* note 655 at art 4(2).
[710] *Ibid* at art 4(4).
[711] *Ibid* at art 9(1).
[712] The special categories include: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
[713] *GDPR, supra* note 655 at art 21(1).
[714] *Ibid.*
[715] *Ibid* at art 22.
[716] *Ibid* at art 23.
[717] *Ibid.*
[718] *Ibid* at arts 4(4), 9(1).

unjust categorizations.[719] Consequently, this creates a situation of exacerbated inequality and increased ability to communicate directly with targeted individuals to influence behaviour.[720] Not only is the goal to manipulate behaviour, but it is also to predict behaviour to forecast outcomes that are likely to create a desired reaction.[721]

One can see how this ability to engage in the panoptic sort could lead to an abuse of surveillance power.[722] For instance, one consequence of the panoptic sort is racial profiling and its effects in the criminal justice system; typically, criminal profiles used by police contain several characteristics in the analysis, but when racial profiling collapses the entire set of characteristics and places a greater weight on the race of the individual, the concern is that several analytical models contain indicators or variables that are biased, and reinforce the bias.[723] For example, when it is assumed that African Americans are more likely to be engaged in criminal behaviour, the consequence is that there are more stops, searches, and arrests, to the point where African Americans are on average subject to significantly more extensive policing.[724]

To be clear, racial profiling occurs in Canada in the same manner as in the United States. Using the same example, the Ontario Human Rights Commission has recently recognized that racial profiling is a systemic problem in policing; both African Canadians and indigenous peoples face systemic discrimination in the criminal justice system.[725] It is established that racial profiling does not work—it is neither efficient nor effective for fighting crime.[726] Still, racial profiling manifests through over-policing.[727] This creates a situation where certain minority groups experience disproportionately more frequent

---

[719] Gandy, Jr, "The Panoptic Sort", *supra* note 699 at 1–2.
[720] *Ibid.*
[721] *Ibid* at 45.
[722] *Ibid* at 15.
[723] Gandy, Jr, "Chance", *supra* note 699 at 124.
[724] *Ibid* at 124–126.
[725] Ontario Human Rights Commission, "Racial Profiling and Human Rights", *Canadian Diversity* 14:1 (2017) 1 at 10 online (pdf): *Ontario Human Rights Commission* <http://www.ohrc.on.ca/sites/default/files/Racial%20Profiling%20and%20Human%20Rights_Canadian%20Diversity.pdf> [Human Rights Commission, "Racial Profiling"].
[726] Ontario Human Rights Commission, "Racial Profiling Doesn't Work" (2020), online: *Ontario Human Rights Commission* <http://www.ohrc.on.ca/en/paying-price-human-cost-racial-profiling/racial-profiling-doesnt-work> [Human Rights Commission, "Does Not Work"].
[727] Human Rights Commission, "Racial Profiling", *supra* note 725 at 11.

contact with police, which is often for less serious matters.[728] Racial profiling can be exhibited through police decisions to stop, question or detain someone; it can also take place prior to a stop and affect the balance of the interaction involving anything from checking a license plate, conducting searches, making arrest decisions, or using force.[729]

Specifically dealing with racial profiling in the information age, a suspicionless stop-and-frisk on the street is one thing, but using power in the cyber domain is another thing altogether; in fact, new forms of racial profiling have been created in subtle ways.[730] This is manifested through predictive policing, sentencing algorithms, targeted hacking tools, and mass surveillance.[731] More precisely, predictive policing aims to prevent crime by predicting where crime will take place next using algorithms that analyze large amounts of data and provide a "heat score" that indicates likelihood of committing a crime; the problem is that the algorithms that are used can have a built-in racial profiling bias, and can additionally be trained on data that is not objective.[732] Similarly, algorithms used to rate each convict to determine the likelihood of recidivism for sentencing purposes may also be biased.[733] Targeted hacking tools can involve hacks into suspects' smartphones, laptops, tablets, internet-connected home devices, and so on, in order to listen in using the built-in microphones or cameras on the devices.[734] It is also technologically possible to conduct mass surveillance of communications using algorithms to automate the process, and machine learning algorithms can be used to engage in predictive policing.[735]

That is not all. Recent reports have surfaced indicating that the RCMP and other police authorities in Canada have been using controversial facial recognition technology, made

---

[728] *Ibid.*
[729] *Ibid.* See also Lorne Foster, Lesley Jacobs & Dr Bobby Siu, "The Ottawa Traffic Stop Race Data Collection Project" in Human Rights Commission, "Racial Profiling" *supra* note 725, 50 at 50−52.
[730] JM Porup, "Racial Profiling in the Information Age" in Human Rights Commission, "Racial Profiling" *supra* note 725, 37 at 37.
[731] *Ibid.*
[732] *Ibid* at 37−38.
[733] *Ibid* at 38.
[734] *Ibid* at 38−39.
[735] *Ibid* at 39.

by a company known as Clearview AI, when conducting police investigations.[736] It appears that some police authorities have admitted to using the technology, and the situation has prompted investigations into the issue.[737] With facial recognition, a type of biometric identification, unique markers are used to identify someone; this is accomplished by using computer algorithms that discern specific distinctive details in a face from a photograph or video, and compare it to data associated with other faces stored in a database in order to find a match.[738] But there are some dangers associated with this technology; some of the main issues that are encountered involve accuracy, the undesired capturing of individuals' sensitive information, misuse and consequent chilling effects, and the disproportionate negative impact on minority groups due to misidentification and racially biased databases stemming from years of racially biased police practices.[739] This means that, not only are minority groups vulnerable because of additional instances of misidentification, but they are also vulnerable due to the presence of biased databases.[740]

Racial profiling is completely unacceptable, and electronic surveillance technology has the potential to magnify its negative effects if there are no checks in place that protect the human dignity of individuals, prevent the abuse of surveillance power, and avoid the negative consequences of profiling.

---

[736] Catharine Tunney, "RCMP's Use of Clearview AI Facial Recognition Technology Under Investigation" (28 February 2020), online: *CBC News* <https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479673>; Andrew Russell, "RCMP Used Clearview AI Facial Recognition Tool in 15 Child Exploitation Cases, Helped Rescue 2 Kids" (27 February 2020), online: *Global News* <https://globalnews.ca/news/6605675/rcmp-used-clearview-ai-child-exploitation/>; Kate Allen, "Toronto Police Chief Halts Use of Controversial Facial Recognition Tool" (13 February 2020), online: *The Star* <https://www.thestar.com/news/gta/2020/02/13/toronto-police-used-clearview-ai-an-incredibly-controversial-facial-recognition-tool.html>; Wendy Gillis & Kate Allen, "Peel and Halton Police Reveal They Too Used Controversial Facial Recognition Tool" (14 February 2020), online: *The Star* <https://www.thestar.com/news/gta/2020/02/14/peel-and-halton-police-reveal-they-too-used-controversial-facial-recognition-tool.html>; Office of the Privacy Commissioner of Canada, "OPC Launches Investigation into RCMP's Use of Facial Recognition Technology" (28 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/>; Office of the Privacy Commissioner of Canada, "Commissioners Launch Joint Investigation into Clearview AI Amid Growing Concerns Over Use of Facial Recognition Technology" (21 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/>.

[737] *Ibid*. As of April, 2020, these investigations have just commenced and are currently active.

[738] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology" (May 2019) at 4−6, online (pdf): *Electronic Frontier Foundation* <https://www.eff.org/files/2019/05/28/face-off-report.pdf>.

[739] *Ibid* at 6−10.

[740] *Ibid.*

This may be why the forward-thinking *Bill SB 6280 (Washington Facial Recognition)* has recently been created to become a groundbreaking law that aims to proactively tackle the problem of law enforcement using facial recognition technology by requiring State and local government agencies to create reports, use a data management policy, minimize inadvertent collection of additional data beyond the amount necessary, use security measures, test prior to deployment, and meet breach notification requirements.[741] More specifically, section 1(1) of *Bill SB 6280 (Washington Facial Recognition)*[742] recognizes the broad social ramifications of the unconstrained use of facial recognition services, and insists that safeguards be put in place to allow State and local government agencies to use the facial recognition services in a manner that benefits society, without threatening individuals' democratic freedoms. Section 2(9) of *Bill SB 6280 (Washington Facial Recognition)*[743] defines "ongoing surveillance" as using a facial recognition service to track the physical movements of a specified individual through one or more public places over time, whether in real time or through application of a facial recognition service to historical records; section 2(10)[744] defines "persistent tracking" as the use of a facial recognition service to track the movements of an individual on a persistent basis without identification or verification of that individual, confirming that tracking becomes persistent as soon as the facial template that permits the tracking is maintained for more than 48 hours after first enrolling that template, or data created by the facial recognition service is linked to any other data such that the individual who has been tracked is identified or identifiable. Furthermore, section 8(1) of *Bill SB 6280 (Washington Facial Recognition),*[745] forces State or local government agencies to disclose their use of facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial.

---

[741] *Bill SB 6280 (Washington Facial Recognition), supra* note 653 at § 3. In my view, Washington State is ahead of many American jurisdictions in that its Constitution, Wash Const art 1, § 7, states that, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law".
[742] *Bill SB 6280 (Washington Facial Recognition), supra* note 653 at § 1(1).
[743] *Ibid* at § 2(9).
[744] *Ibid* at § 2(10).
[745] *Ibid* at § 8(1).

What is most essential for the purposes of this discussion is section 11 of *Bill SB 6280 (Washington Facial Recognition),*[746] because meaningful limits have been put in place to prevent the abuse of electronic surveillance power, and in particular, the dangerous inevitable consequences of profiling. More specifically, pursuant to section 11(1) of *Bill SB 6280 (Washington Facial Recognition),*[747] State or local government agencies are not allowed to use a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless: a warrant is obtained authorizing the use of the service for those purposes; exigent circumstances exist; or a court order is obtained authorizing the use of the service for the sole purpose of locating or identifying a missing person, or identifying a deceased person. Moreover, section 11(2) of *Bill SB 6280 (Washington Facial Recognition)*[748] makes it clear that it is prohibited to apply a facial recognition service to any individual based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law—it specifically states that "this subsection does not condone profiling including, but not limited to, predictive law enforcement tools".[749] And section 11(5) of *Bill SB 6280 (Washington Facial Recognition)*[750] states that State or local law enforcement agencies cannot use the results of a facial recognition service as the sole basis to establish probable cause in a criminal investigation; the results can only be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation. Also, section 11(7) of *Bill SB 6280 (Washington Facial Recognition)*[751]prohibits substantively manipulating an image for use in a facial recognition service in a manner that is inconsistent with the facial recognition service provider's intended use.

---

[746] *Ibid* at § 11.
[747] *Ibid* at § 11(1).
[748] *Ibid* at § 11(2).
[749] *Ibid.*
[750] *Ibid* at § 11(5).
[751] *Ibid* at § 11(7).

What the foregoing suggests is that it is critical to have limits in place that prevent ongoing, persistent, or real-time electronic surveillance, and also acts of profiling and predictive policing. As well, boundaries are established so that facial recognition technology cannot be used on its own; any results must be used in conjunction with other lawfully obtained pieces of information for the purposes of a criminal investigation.

These ideas are clearly applicable in the context of State and local government, with a focus on the criminal law context; however, I would like to suggest that they can be borrowed from this context and tailored to the employment context. That is, the definitions and prohibitions can act as a guide for the purposes of drafting provisions in the new workplace privacy regime. In my view, the concepts discussed above, together with the above discussion of the concepts in the *GDPR*, can be instructive; this is especially true regarding ongoing surveillance, persistent tracking, prohibitions against using the surveillance technology unless certain rare conditions are met, prohibitions against applying electronic surveillance technology to special groups of individuals or categories of sensitive personal data, using the results of the electronic surveillance technology as the sole basis in the decision-making process, profiling, and predictive decision-making that are all important to consider when creating the workplace privacy regime. Considering these essential facets of electronic surveillance during the drafting process can introduce additional dimensions to the discussion when creating a new workplace privacy regime.

Let me pause for a moment to recap my argument to this point. I have explained how there are some issues with *PIPEDA's* definitions and conceptualizations, and this creates complications with respect to dealing with the electronic surveillance gap. I also examined approaches used by other jurisdictions to glean information that can help me to close the electronic surveillance gap.

What I would like to do now is delve into Schedule 1 of *PIPEDA,*[752] which contains the Fair Information Principles set out in the CSA Standard.[753]

---

[752] *PIPEDA*, *supra* note 643 at Schedule 1.

These Principles set out 10 obligations that must be complied with by all organizations.[754] While these Principles were appropriate back in 1980 when the *OECD Privacy Guidelines*[755] were first created, in 1996 when the CSA Standard[756] was created based on those guidelines, and in 2000−2001 when *PIPEDA* took effect,[757] I would like to suggest that they are no longer sufficient as they currently are for Canada's privacy regime. That is, it may be precarious to assume that the fine technological intricacies of electronic surveillance and their implications would have been sufficiently appreciated in 1980, 1996, or even 2001 for that matter.

And when it comes to employment, I argue that there is a serious electronic surveillance gap that needs to be closed in this regard. Since provisions addressing concerns regarding electronic surveillance in employment are simply not explicated anywhere in the legislation, I believe that it is necessary to address this problematic issue of the electronic surveillance gap in employment immediately.

---

[753] Canada Standards Association, "CSA Standard CAN/CSA-Q830, Model Code for the Protection of Personal Information" (March 1996), online (pdf): *Canada Standards Association* <https://simson.net/ref/1996/CSA_Privacy_Standard_CSA-Q830-96.pdf> [CSA Standard]. See also Pam Dixon, "A Brief Introduction to Fair Information Practices" (5 June 2006), online: *World Privacy Forum* <https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>; Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principles" (May 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>.

[754] *Ibid; PIPEDA, supra* note 643 at s 5(1). Section 5(1) states that, subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1. Section 5(2) states that, when the word, "should", is used in the Schedule, it indicates a recommendation and not an obligation. The 10 principles are: (1) Accountability; (2) Identifying Purposes; (3) Consent; (4) Limiting Collection; (5) Limiting Use, Disclosure, and Retention; (6) Accuracy; (7) Safeguards; (8) Openness; (9) Individual Access; and (10) Challenging Compliance.

[755] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980), online: *OECD* <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>;OECD, "The OECD Privacy Framework" (2013), online (pdf): *OECD* <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [*OECD Privacy Guidelines*].

[756] Canada Standards Association, *supra* note 753.

[757] *PIPEDA, supra* note 643. Parts 2, 3 and 4 became effective on May 1, 2000 and Part 1 (with section 5 that refers to the need to comply with Schedule 1) took effect on January 1, 2001. Part 5 became came into force on June 1, 2009.

For instance, when examining Canada's Principle 4 in clause 4.4 of Schedule 1 of *PIPEDA,*[758] we see that the way in which collection has been envisioned and set out in the legislation cannot effectively address electronic surveillance challenges that may arise. Principle 4 in Schedule 1 of *PIPEDA*[759] has three clauses discussing limiting collection, following an opening that requires that collection be limited to what is necessary for the purposes, and information be collected by fair and lawful means. First, clause 4.4.1[760] prevents personal information from being collected indiscriminately, requiring that the amount and type of information collected is limited to what is necessary to fulfill the purposes that are identified; organizations must specify the type of information collected in accordance with their policies and procedures. Second, clause 4.4.2[761] requires personal information to be collected by fair and lawful means in order to prevent organizations from collecting information by misleading and deceiving individuals about the purpose for which the information is collected; the clause also states that there is an implied requirement that consent to the collection is not obtained through deception. Third, clause 4.4.3[762] states that limiting collection is linked to two other principles involving purposes and consent.[763]

Again, no discussion of electronic surveillance is included under Principle 4 in clause 4.4 of Schedule 1 of *PIPEDA.*[764] In my view, while the existing clauses may be helpful in general situations involving data collection, they would not be instructive in situations involving electronic surveillance, and certainly not ones involving employment, since some problematic assumptions have been made.

The first problematic assumption is that employees are able to provide, withhold, or revoke consent to the collection in the first place; clauses 4.4.2[765] and 4.4.3[766] specifically

---

[758] *PIPEDA, supra* note 643 at Schedule 1, cl 4.4.
[759] *Ibid*.
[760] *Ibid* at cl 4.4.1.
[761] *Ibid* at cl 4.4.2.
[762] *Ibid* at cl 4.4.3.
[763] Consent will be discussed next in Theme 2, and purposes will be discussed in this theme as it becomes relevant to this discussion.
[764] *PIPEDA, supra* note 643 Schedule 1, cl 4.4.
[765] *Ibid* at cl 4.4.2.
[766] *Ibid* at cl 4.4.3.

refer to the need to obtain consent in a manner that is not misleading or deceiving about the purposes of the collection, which must be necessary. Issues of consent and employees' ability to consent will be tackled in Theme 2. What is important to note at this point is that Principle 4 involving collection[767] is in the majority of cases unworkable in the employment context in relation to the concept of consent; I will be arguing that employees are in most cases not in a position to provide, withhold, or revoke consent, and some other strategy is necessary to close the electronic surveillance gap.[768]

The second assumption, which I will address here, is that clause 4.4.2[769] is sufficient to prevent organizations that are collecting personal information from engaging in function creep in situations involving electronic surveillance. Function creep involves the repurposing of personal information for new uses without the knowledge of the owner of the data.[770] Function creep carries a high potential for abuse of electronic surveillance power, given that employees are the more vulnerable party and employers have the power to use technology to their advantage as the overseer with heightened visibility.[771] This is critical in the employment context, given the detrimental effects of excessive monitoring on employees.[772] One major concern among employees is that personal information that is collected exclusively for one reason (for instance, to protect company property) could be used for another reason (for example, to make disciplinary decisions following a discovery of a breach of company rules).[773]

---

[767] *Ibid* at cl 4.4.
[768] See the discussion in Theme 2. For the rare situations where consent might apply in the employment context, I assert that still, Principle 4 is not capable of closing the electronic surveillance gap because there are additional reasons why it would not be helpful in situations involving electronic surveillance in the employment context, as described below.
[769] *PIPEDA*, *supra* note 643 at Schedule 1, cl 4.4.2.
[770] Mark Andrejevic, "Big Data Era", *supra* note 688 at 67–68.
[771] Shoshana Zuboff, "Smart Machine", *supra* note 700 at 324–327.
[772] Kirstie Ball, "Workplace Surveillance: An Overview" (2010) 51:1 Labor History 87 at 93−94, online (pdf): *tandfonline* <www.tandfonline.com> DOI: <10.1080/00236561003654776> [Kirstie Ball, "An Overview"].
[773] Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance, WP 48" (11 February 2004) at 24−25, online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf> [Working Party, "Opinion 4/2004"].

It might be objected that this problem is addressed under identifying purposes under Principle 2 in clause 4.2 of Schedule 1 of *PIPEDA*.[774] Under clause 4.2.2,[775] the purposes for which personal information is collected must be identified by the organization at or before the time the information is collected, in order to determine the information that is required to be collected to fulfil these purposes. Moreover, clause 4.2.4[776] states that, when personal information that has been collected is to be used for a purpose not previously identified, the new purpose must be identified prior to use, because the consent of the individual would be required for this new purpose.[777]

In response I would simply point out that clauses 4.2.2[778]and 4.2.4[779] are insufficient for addressing current pressures to engage in function creep in light of the unequal bargaining power of the parties.[780] This is because they do not take into account the sophistication of electronic surveillance technologies, and underestimate the simplicity of repurposing surveillance information.[781] In my view, the unequal bargaining power of the parties, together with the elaborate technological capabilities of electronic surveillance, creates a situation where it could be effortless to find ways to take advantage and engage in function creep. Again, there is the problematic assumption that consent is something that employees can provide, withhold, or revoke; in clause 4.2.4,[782] there is a requirement to obtain consent before information can be used for new purposes.[783]

The third problematic assumption is that clause 4.4.1 in Principle 4 of Schedule 1 of *PIPEDA*[784] is sufficient for dealing with situations involving electronic surveillance. In my view, the risk in employment is that employers, the dominant party in the relationship, would take advantage of their electronic surveillance power if these were the

---

[774] *PIPEDA, supra* note 643 at Schedule 1, cl 4.2.
[775] *Ibid* at cl 4.2.2.
[776] *Ibid* at cl 4.2.4.
[777] *Ibid*. This rule would not apply in situations where the new purpose is required by law.
[778] *PIPEDA, supra* note 643 at Schedule 1, at cl 4.2.2.
[779] *Ibid* at cl 4.2.4.
[780] Shoshana Zuboff, "Smart Machine", *supra* note 700 at 324–327.
[781] Mark Andrejevic, "Big Data Era", *supra* note 688 at 67–68.
[782] *PIPEDA, supra* note 643 at Schedule 1, at cl 4.2.4.
[783] See the discussion in Theme 2.
[784] *PIPEDA, supra* note 643 at Schedule 1, at cl 4.4.1.

only limits in place, and could gather and accumulate surveillance information that goes well beyond the parameters of "amounts and types of information" in clause 4.4.1.[785] I therefore conclude that clause 4.4.1[786] is insufficient and cannot be used to close the electronic surveillance gap.

More precisely, one must consider the four temporal dimensions for a complete understanding of any instance of surveillance: the timeframe in which the surveillance is conducted (ephemeral, across a single span of time, across recurrent spans such as within 24-hour cycles, or scattered across time following a trigger); the intensity with which surveillance is conducted (once, repeated, or continuous); the persistence of consequences of surveillance (ephemeral because it is limited to observation, short-to-medium term because it is recorded, or long-term or permanent because it is archived); and the time period within which surveillance is applied (the present, real-time use, the past through retrospective use, or the future through prospective or predictive use).[787] Without proper boundaries in place for the watchers, the surveillance efforts have the potential to be overgeneralized and begin too broadly in hopes of finding a problem, rather than beginning with a reason to be searching in the first place.[788]

In light of the above discussion, it may be beneficial to borrow the *GDPR* principles of purpose limitation,[789] which states that personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, and data minimization,[790] which states that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. These provisions appear to have more depth and place more appropriate limits on the watchers.

---

[785] *Ibid*.
[786] *Ibid*.
[787] Clarke & Greenleaf, *supra* note 682 at 108–109.
[788] Mark Andrejevic, "Big Data Era", *supra* note 688 at 58.
[789] *GDPR*, *supra* note 655 at art 5(b).
[790] *Ibid* at art 5(c).

As the above analysis illustrates, *PIPEDA* lacks clarification relating to electronic surveillance issues in the employment context. The kinds of provisions that are required for regulating electronic surveillance in the workplace do not currently exist in *PIPEDA*; I would like to suggest that, in order to close the electronic surveillance gap, it is imperative to add several new provisions that specifically address the dangers associated with this sophisticated technology when it comes to employment.

To recap my argument to this point, I first showed that there are some difficulties with *PIPEDA's* definitions and conceptualizations, and I then demonstrated that there are problems with Schedule 1 of *PIPEDA*[791] with respect to addressing electronic surveillance issues in the employment context. The third thing that I will do is stress that, given the above-mentioned gaps, it is vital to build trust with respect to this new workplace privacy regime; indeed, trust is essential when addressing privacy concerns[792] in the workplace,[793] and it is especially necessary if the goal is to encourage Canadians to adopt a new workplace privacy regime.[794] In this part, I will argue that, when examining other jurisdictions, we can identify several strategies that can be used in order to build trust in the new workplace privacy regime.

The first place to start is by examining the purpose of the legislation. In Canada, section 3 of *PIPEDA*[795] pragmatically recognizes the need to balance the right of privacy of individuals with the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[796] However, there is currently no reference to fundamental rights and freedoms; instead, it incorporates the question of what a reasonable person would consider to be appropriate in the circumstances.[797]

---

[791] *PIPEDA*, *supra* note 643 at Schedule 1.
[792] Waldman, *supra* note 703 at 93–99.
[793] Kirstie Ball, "An Overview", *supra* note 772 at 89.
[794] Geist, *supra* note 659 at 23m:28s−23m:41s.
[795] *PIPEDA*, *supra* note 643 at s 3.
[796] *Ibid.* This strategy of considering reasonable expectations in the circumstances appears to be more in line with the pragmatic approach to privacy, and not a rights-based approach. See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010) at 1–2, 231–233.
[797] *PIPEDA*, *supra* note 643 at s 3.

In contrast, Article 1 of the *GDPR*[798] expressly states that the *GDPR* protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[799] In my view, Canada should do the same, and if Canada intends to use a dignity/human rights approach to privacy in its private sector data protection legislation, it should be recognizing that dignity is critical when dealing with personal data of Canadians.[800] For Canadians to feel included and experience a sense of fairness and empowerment,[801] they must be shielded with data protection provisions that explicitly refer to fundamental rights and freedoms.

There are a few more ways to ensure that there is increased trust in the new workplace privacy regime, so that individuals can more effectively deal with the uncertainty and complexity of privacy concerns in modern times.[802]

One such way is to borrow some noteworthy features from Article 25(1) and (2) of the *GDPR*,[803] which sets data protection as the default and requires controllers to take steps to ensure that processing is carried out with appropriate measures and safeguards in place. Although there is currently a policy to this effect in Canada, by Ann Cavoukian,[804] entitled, "Privacy by Design",[805] I would like to suggest that there should be an explicit legislative provision in *PIPEDA* that includes Cavoukian's ideas. I am not alone with this contention; in February 2018, the Standing Committee on Access to Information, Privacy and Ethics recommended that *PIPEDA* be amended to make privacy by design a central principle and to include the seven foundational principles of this concept, where

---

[798] *GDPR*, *supra* note 655 at art 1.
[799] *Ibid.*
[800] Edward J Bloustein, *Individual & Group Privacy* (London: Transaction Publishers, 2003) at 44−46.
[801] Hicks, *supra* note 702 at 16–17.
[802] Waldman, *supra* note 703 at 74.
[803] *GDPR*, *supra* note 655 at art 25(1)−(2).
[804] Privacy by Design Centre of Excellence, "Dr. Ann Cavoukian, Distinguished Expert-in-Residence" (2020), online: *Ryerson University* <https://www.ryerson.ca/pbdce/about/ann-cavoukian/>. Ann Cavoukian served an unprecedented three terms as Information and Privacy Commissioner of Ontario.
[805] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles" (January 2011), online (pdf): *Office of the Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

possible.[806] Briefly, the seven principles include: (1) Proactive not Reactive; Preventative not Remedial; (2) Privacy as the Default Setting; (3) Privacy Embedded into Design; (4) Full Functionality — Positive-Sum, not Zero-Sum; (5) End-to-End Security — Full Lifecycle Protection; (6) Visibility and Transparency — Keep it Open; and (7) Respect for User Privacy — Keep it User-Centric.[807] In my view, this can apply and be tailored to the employment context.

Another way to build trust is to borrow from Article 35(1) and 35(7) of the *GDPR*,[808] stating that, where processing, particularly in respect of new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller must perform an assessment before processing of the impact of the processing operations on the protection of personal data; there are several factors to consider when completing the assessment, including the processing operations, legitimate interests, necessity and proportionality of processing in relation to the purposes, risks to rights and freedoms, and measures used to address the risks.[809]

And another way that Canadians can build trust in the system is to incorporate language that is rights-based directly into the data protection legislation.[810] In my view, this goal is necessary and achievable for three reasons. The first reason is because in Canada, we see the shift toward an acknowledgment of the importance of a right to privacy, which is in line with other jurisdictions. More specifically, Québec has created a right to private life,

---

[806] Bob Zimmer, "Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics (February 2018) at 50–52, online (pdf): *House of Commons* <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>.
[807] Cavoukian, *supra* note 805.
[808] *GDPR*, *supra* note 655 at art 35(1), (7).
[809] See Theme 2 for an in-depth discussion on legitimate interests, necessity, and proportionality.
[810] Office of the Privacy Commissioner of Canada, "2018–2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act"*(10 December 2019) at 11−18, online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf> [Privacy Commissioner, "2018–2019 Annual Report"]. For instance, the following are key words and phrases that could be included in a new regime: fundamental rights and freedoms; dignity; self-respect; autonomy; basic human right; privacy rights; proportionality; and rights and freedoms balanced with legitimate interests.

as described in section 5 of the *Québec Charter*.[811] The right is broadly constructed and simply stated, highlighting that every person has a right to private life.[812] It is comparable to California's section 1 of Article 1 of the *California Constitution*[813] that states that all people are by nature free and independent and enjoy inalienable rights, one of which is privacy. What is more, Article 8(1) of the *EU Convention*[814] has a relatively wider scope, given that it includes protections associated with privacy and electronic surveillance, and includes private life, family life, home, and correspondence.[815] There is also a balancing provision in Article 8(2) of the *EU Convention*,[816] to prevent interferences with the exercise of the right, except in rare specified situations such as national security or public safety. Article 8 of the *EU Convention*[817] has been constructed broadly to enable a more organic and flexible approach to understanding current concerns regarding electronic surveillance in an evolving society.[818] The openness of the language also allows for a liberal and purposive interpretation; at the same time, it provides for exceptions to be narrowly construed and an explicit balancing mechanism to ensure fairness.[819]

The common denominator of the above provisions is that they emphasize the importance of treating all persons as worthy of honour and respect in accordance with the dignity/human rights theoretical approach to privacy.[820] All persons are deserving of this right because they are equal in status whereby no one person is better than another.[821] Pursuant to the dignity/human rights perspective, privacy is viewed as an essential human need.[822] By virtue of being human, we need to have some degree of privacy, and this is

---

[811] *Québec Charter*, *supra* note 642 at s 5.
[812] *Ibid.*
[813] *California Constitution*, *supra* note 648 at § 1.
[814] *EU Convention*, *supra* note 654 at art 8.
[815] *Ibid* at art 8(1).
[816] *Ibid* at art 8(2).
[817] *Ibid* at art 8.
[818] Ruth Sullivan, *Sullivan on the Construction of Statutes*, 5th ed (Markham, Ontario: LexisNexis Canada Inc, 2008) at 255−297, 497−507.
[819] *Ibid; EU Convention*, *supra* note 654 at art 8(2). Interpretation of Article 8 will be elaborated upon in Chapter 5, where workplace privacy cases involving electronic surveillance are analyzed concerning private life and correspondence.
[820] Alexandra Rengel, *Privacy in the 21st Century* (Netherlands: Koninklijke Brill, 2013) at 1; Stenson, *supra* note 666 at *sub verbo* "dignity".
[821] George Kateb, *Human Dignity* (Cambridge: Harvard University Press, 2011) at 5–9.
[822] Rengel, *supra* note 820 at 1.

natural and intrinsic.[823] Individuals are to be treated as ends in themselves rather than as means to furthering another person's or society's goals.[824] Without the human right to privacy, the autonomy of individuals would be threatened and this is troubling since autonomy is necessary to have a sense of liberty to pursue aims without interference.[825]

In line with this reasoning, recent decisions of the Supreme Court of Canada have emphasized the importance of privacy for the flourishing of a free and democratic society; in fact, it has referred to the right to privacy in the broadest sense to include several aspects including secrecy, control-over-information, access to information, and anonymity.[826] The Supreme Court of Canada has stressed that privacy is essential for a person's sense of dignity and autonomy, and involves freedom from unwanted scrutiny, intrusion or attention (including through observation or recording).[827] Furthermore, the Supreme Court of Canada has recognized that, "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives".[828]

The second reason is because privacy has historically been considered a quasi-constitutional right in public sector privacy cases regarding data protection laws,[829] and has also recently been acknowledged by the Supreme Court of Canada as an important quasi-constitutional right when deciding on private sector privacy cases regarding data

---

[823] *Ibid.*
[824] Chris D L Hunt, "Conceptualizing Privacy and Elucidating Its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2001) 37 Queen's LJ 167 at 203−204.
[825] James Griffin, "The Human Right to Privacy" (2007) 44 San Diego L Rev 697 at 700.
[826] *R v Spencer*, 2014 SCC 43 at paras 34−47; *R v Jarvis*, 2019 SCC 10 at paras 28−30, 36; *R v Jones*, 2017 SCC 60 at paras 35−45 [*Jones*]. Note that interpretations of section 5 of the *Québec Charter* are in line with these conceptualizations of privacy, as a broad right that includes elements of autonomy, dignity, a sense of control, and integrity of the individual, along with a right to one's image. However, in Québec, section 49 of the *Québec Charter* states that any interferences with a right entitles the victim to obtain cessation of the interference and also compensation for the moral or material prejudice resulting therefrom due to civil law principles of recovery associated with the statute. See *Aubry c Éditions Vice Versa Inc*, [1998] 1 SCR 591, at paras 21, 49, 52−53, 66−70, 1998 CarswellQue 4806 (SCC) [*Aubry*].
[827] *Ibid.*
[828] *Jones, supra* note 826 at para 45.
[829] The public sector privacy legislation, *Privacy Act*, RSC, 1985, c P-21, has been considered to be quasi-constitutional as seen in *Lavigne v Canada (Commissioner of Official Languages)*, 2002 SCC 53 at para 24; *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403, at paras 65-66, 132 FTR 55 (SCC); *HJ Heinz Co of Canada Ltd v Canada (Attorney General)*, 2006 SCC 13 at para 28. See also Michael E Power, *The Law of Privacy* (Markham: LexisNexis Canada Inc, 2013) at 13; Marta Otto, *The Right to Privacy in Employment: A Comparative Analysis* (Oxford: Hart Publishing, 2016) at 133−134.

protection laws.[830] But in my view, the nature of quasi-constitutional status of rights is not well understood or given due consideration in Canada, since it is complicated and confusing to fully grasp a right that is not quite constitutional but more than ordinary, and this leads to a lack of clarity for Canadians.[831] I believe that Canada needs to be bold, move in the same direction as the other jurisdictions that are being studied in this dissertation, and go beyond what is currently provided; one way to achieve this goal is to explicitly create right-based data protections in *PIPEDA*.

The third reason is because there has been a previous attempt to create a constitutional right to privacy in Canada, which would have included a freedom from surveillance. More precisely, on March 13, 2001, Senator Sheila Finestone introduced *Bill S-21 (Privacy Rights Charter)*[832] in the Canadian Senate.[833] The purpose had been to establish a right to privacy for individuals, including: physical privacy; freedom from surveillance; freedom from monitoring or interception of their private communications; and freedom from the collection, use, and disclosure of their personal information.[834] No person would have been allowed to unjustifiably infringe on an individual's right to privacy, and individuals would have been entitled to claim and enforce their right to privacy; an infringement would have been justifiable if it was reasonable and could be demonstrably justified in a free and democratic society.[835] There would have been a four-part test for justifiable infringements; also, the interference would have been considered to be not infringing if there was free and fully informed consent.[836] However, the Standing Senate Committee on Social Affairs, Science and Technology had several concerns about how *Bill S-21 (Privacy Rights Charter)* would practically work with Canada's existing laws,

---

[830] *UFCW, Local 401 v Alberta (Information and Privacy Commissioner)*, 2013 SCC 62 at para 19; *Douez v Facebook Inc*, 2017 SCC 33 at paras 58–59.
[831] Vanessa MacDonnell, "A Theory of Quasi-Constitutional Legislation" (2016) 53 Osgoode Hall LJ 508 at 509, 527.
[832] *Bill S-21(Privacy Rights Charter), supra* note 647 at s 1.
[833] Parliament of Canada, "S-21, An Act to Guarantee the Human Right to Privacy" (2001–2002), online: *Parliament of Canada* <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=4772262&View=0>.
[834] *Bill S-21(Privacy Rights Charter), supra* note 647 at s 3.
[835] *Ibid* at ss 4(1), 4(3), 5(1)−(2).
[836] *Ibid* at s 5(3)−(4).

and recommended further study.[837] Ultimately, *Bill S-21 (Privacy Rights Charter)* was dropped from the Senate Order Paper on April 16 2002.[838]

What the foregoing suggests is that the law needs to adapt to evolving societal values and embrace the idea of including rights-based language in data protections provisions. The times have changed: technological capabilities, potential dangers, and societal attitudes have evolved.[839] The lawmakers and policymakers must respond.

One further way to build trust is to borrow and adapt a feature that has recently surfaced in a bill proposed in the United States, namely in section 1102 of *Bill S5642 (New York Privacy Act)*[840] dealing with the idea of a data fiduciary.

While *Bill S5642 (New York Privacy Act)* applies to the consumer context,[841] the concept of a data fiduciary could be adapted to fit the employment context. Employees are vulnerable and are in particular need of the very type of protection that is contemplated with the introduction of the data fiduciary in light of the blurring of workplace and personal digital devices as well as a blurring of work and personal time.[842]

---

[837] The Standing Senate Committee on Social Affairs, Science and Technology, "Report of the Committee" (14 December 2001), online: *Senate of Canada* <https://sencanada.ca/Content/SEN/Committee/371/soci/rep/rep13dec01-e.htm>. The main concerns were: the proposed changes could harm the work of law enforcement agencies because their activities and standards were already approved by Parliament or the courts; there could be excessive litigation as a result of the changes; the role of the Privacy Commissioner was not clear; there could be a consequent parallel complaints process established and potential danger of competing rulings resulting from litigation and the Privacy Commissioner; there could be consequent credibility problems between *PIPEDA* and *Bill S-21 (Privacy Rights Charter)*; the application could be problematic; the proposed provisions could confuse or obstruct approaches taken by courts when applying the *Canadian Charter of Rights and Freedoms*, s 7, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982*(UK),1982, c 11 [*Canadian Charter*]; and the proposed provisions could create uncertainty when interacting with the *Canadian Charter*, *Canadian Human Rights Act*, RSC, 1985, c H-6, the *Criminal Code*, RSC, 1985, c C-46, or the *Official Languages Act*, RSC, 1985, c 31 (4th Supp).

[838] Parliament of Canada, *supra* note 833.

[839] Brad Smith & Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press, 2019) at 1−151; CNN Business, "Microsoft President: There is a privacy crisis" (11 October, 2019) online (video): *CNN Business* <https://www.cnn.com/videos/business/2019/10/11/brad-smith-microsoft-privacy-laws-boss-files-orig.cnn-business/video/playlists/business-boss-files/>.

[840] *Bill S5642 (New York Privacy Act)*, *supra* note 652 at § 1102.

[841] *Ibid* at § 1101.

[842] *Machtinger v HOJ Industries Ltd*, [1992] 1 SCR 986 at para 31, 1992 CarswellOnt 892 (SCC) [*Machtinger*]; *Wallace v United Grain Growers Ltd*, [1997] 3 SCR 701 at paras 92−93, 1997 CarswellMan 455 (SCC) [*Wallace*]. See also David J Doorey, *The LAW of Work: Common Law and the Regulation of Work* (Toronto: Emond Montgomery Publications Limited, 2016) at 5−6, 67−75, 111−120 [David Doorey,

Employers have an obligation of good faith and fair dealing in the course of dismissals, which at minimum requires employers to be candid, reasonable, honest and forthright with their employees and should refrain from engaging in conduct that is unfair or is in bad faith by being, for example, untruthful, misleading or unduly insensitive.[843] In like manner, I believe that it may be possible to augment this duty of good faith by adding carefully defined obligations related to data protection. For this idea to be workable, employers would need to focus on more than just their own business goals of maximizing human capital and generating profits.[844]

Let me begin with a definition of "fiduciary", which means "involving trust, especially with regard to the relationship between a trustee and a beneficiary: the company has a fiduciary duty to its shareholders"; it comes from the Latin "*fiduciarius*", from "*fiducia*", meaning "trust" and "*fidere*", meaning "to trust".[845] When it comes to understanding the

---

"Common Law and Regulation"]; David J Doorey, *The LAW of Work: Industrial Relations and Collective Bargaining* (Toronto: Emond Montgomery Publications Limited, 2017) at 67, 94−97, 239−241[David Doorey, "Industrial Relations and Collective Bargaining"]; Elizabeth Denham, "The Employment Relationship as the Privacy Laboratory" (22 November 2013), online: *Office of the Information and Privacy Commissioner for British Columbia* <https://www.oipc.bc.ca/speeches/1584> at 2–3, 5–10; Government of Canada, "Disconnecting From Work-Related E-Communications Outside of Work Hours: Issue Paper" (4 April 2019), online: *Government of Canada* <https://www.canada.ca/en/employment-social-development/services/labour-standards/reports/disconnecting-e-communications.html>; Office of the Privacy Commissioner of Canada, "Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?" (22 July 2015), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/> [Privacy Commissioner, "BYOD Program the Right Choice?"]; Lysa Appleton, "Flex Work and Telecommuting" (2018), online: *Career Professionals of Canada* <https://careerprocanada.ca/flex-work-telecommuting/>; Nathan Battams, "Out of the office: workshifting and remote work in Canada" (August 2013) at 1, online (pdf): *The Vanier Institute: Fascinating Families* <http://vanierinstitute.ca/wp-content/uploads/2015/11/FFAM_2013-08-00_Workshifting-and-remote-work-Canada.pdf>; Jennifer Stoddart, "Annual Reports to Parliament 2004 on the Personal Information Protection and Electronic Documents Act" (October 2005), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/200405/2004_pipeda/>.

[843] *Wallace*, *supra* note 842 at para 98.

[844] Peter Kivisto, *Social Theory: Roots & Branches*, 5th ed (Oxford: Oxford University Press, 2013) at 3–38; Carsten Bagge Laustsen et al, *Social Theory: A Textbook* (London: Routledge, 2017) at 14−34, online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315657998>; Nick Dyer-Witheford, *Cyber-Proletariat: Global Labour in the Digital Vortex* (Toronto: Between the Lines, 2015) at 4−15, 19−38.

[845] Stenson, *supra* note 666 at *sub verbo* "fiduciary".

nature of a fiduciary duty, there are differing approaches on the content of such a duty; the more common narrow approach includes proscriptive duties such as the no-profit rule and the no-conflict rule, whereas the broad approach may include additional duties such as the duty of good faith and the duty of confidence.[846] The boundaries may be poorly defined, but there is consensus on its essence; the core element of the fiduciary duty is the duty of loyalty.[847] That is, fiduciaries must act faithfully toward their beneficiaries.[848] More specifically, fiduciaries must not engage in disloyal conduct grounded in self-interest.[849] Another aspect is a conflict of duty rule that prohibits fiduciaries from acting under conflicting mandates, even if the conflicting duties involve two different third parties.[850] In fiduciary relationships, the fiduciary exercises discretionary power over the practical interests of the beneficiary; this power is a type of authority derived from the legal capacity of the beneficiary or a benefactor that ensures the proper exercise of the power.[851] These fiduciary duties are strict due to the reprehensibility of self-interested conduct, even if the beneficiary has suffered no losses; this could be in order to discourage the temptation of selfish behaviour in fiduciaries and to protect vulnerable persons against the abuse of their trust and confidence in others.[852]

What is most relevant to this discussion is that section 1102(1) of *Bill S5642 (New York Privacy Act)*[853] creates a requirement to meet the duties of care, loyalty, and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk, and must act in the best interests of the consumer without regard to any self-interests, in a manner expected by a reasonable consumer under the circumstances. Risk is defined broadly in section 1102(2) of *Bill S5642 (New York Privacy Act)*[854] to include many kinds of harm, some of which include: financial

---

[846] Remus Valsan, "Fiduciary Duties, Conflict of Interest, and Proper Exercise of Judgment" (2016) 62:1 McGill LJ 3 at 9−11.
[847] Paul B Miller, "Justifying Fiduciary Duties" (2013) 58 McGill LJ 969 at 976.
[848] *Ibid.*
[849] *Ibid.*
[850] *Ibid.*
[851] *Ibid* at 1021−1023.
[852] Valsan, *supra* note 846 at 11−12.
[853] *Bill S5642 (New York Privacy Act), supra* note 652 at § 1102(1).
[854] *Ibid* at § 1102(2).

harm, physical harm, psychological harm, and even adverse employment outcomes. Section 1102(1) of *Bill S5642 (New York Privacy Act)*[855] lists various strict and detailed prohibitions related to the three duties of care, loyalty, and confidentiality.

Some of the duties seem to be more practical to implement than others. For instance, the duty of care appears to be familiar to Canadians given the requirements regarding safeguards and breach reporting;[856] however, the duty of loyalty, which is noted above as the core essence of the fiduciary duty, is seemingly more challenging to meet, especially in the employment context.[857] In particular, the provision prohibits the fiduciary from using personal data or data derived from personal data in a way that benefits the fiduciary to the detriment of a user, and will either result in reasonably foreseeable and material physical or financial harm to a consumer, or would be unexpected and highly offensive to a reasonable consumer.[858] I anticipate that there could be some interpretation issues with this requirement concerning what constitutes "detriment", "reasonably foreseeable", and "material harm".

Even more challenging is the duty of confidentiality, which outlines requirements of: not disclosing or selling to, or sharing personal data with, any other person except as consistent with the duties of care and loyalty; not disclosing or selling to, or sharing personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed; and taking reasonable steps to ensure that the practices of any person to or with whom the fiduciary discloses, sells, or shares personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.[859] In my view, though the first requirement to operate in line with the duties of care and loyalty seems realistic, the rule

---

[855] *Ibid* at § 1102(1).
[856] *PIPEDA, supra* note 643 at ss 10.1−10.3, Schedule 1, cl 4.7; *Bill S5642 (New York Privacy Act), supra* note 652 at § 1102)1)(a).
[857] *Bill S5642 (New York Privacy Act), supra* note 652 at § 1102(1)(b).
[858] *Ibid.*
[859] *Ibid* at § 1102(1)(c).

requiring organizations to form a contract and demand that others operate in accordance with these duties, and then regularly audit them to confirm compliance, appears to be too onerous for most to meet. To be fair, I can appreciate why there have been strong responses from technology companies in this regard.[860]

Another section that appears challenging to implement is section 1102(3) of *Bill S5642 (New York Privacy Act),*[861] which states that this fiduciary duty supersedes any duty owed to owners or shareholders. This could have serious implications given the enforcement provisions of *Bill S5642 (New York Privacy Act)*[862] that refer to unfair or deceptive acts in trade or commerce and unfair methods of competition, and set out rights of action that are granted to any governmental body to enforce the section, or any person who has been injured to bring an action for damages or an injunction.

In this part, my goal was to argue that *PIPEDA* contains significant gaps and does not sufficiently address issues related to electronic surveillance; moreover, other jurisdictions provide instructive information that can help to fill the identified gaps. I achieved this goal by showing that there were problems with *PIPEDA's* definitions and conceptualizations, and with several provisions in Schedule 1 of *PIPEDA*[863] when it came to dealing with issues involving electronic surveillance in the employment context. I emphasized that it was therefore necessary to create new provisions to address these concerns and also find novel ways to enhance trust in the new workplace privacy regime.

4.1.3 Implications for the New Workplace Privacy Regime

To conclude this section, I have argued that the meaning of collection and processing is not well articulated in *PIPEDA* and needs to be clarified. I pointed out that *PIPEDA* does not sufficiently address issues of electronic surveillance and the negative consequences of profiling, and this will require new provisions in order to address electronic surveillance challenges more specifically. There is also a need to build trust in this privacy regime;

---

[860] Issie Lapowsky, "New York's Privacy Bill Is Even Bolder Than California's" (4 June 2019), online: *Wired* <https://www.wired.com/story/new-york-privacy-act-bolder/>.
[861] *Bill S5642 (New York Privacy Act), supra* note 652 at § 1102(3).
[862] *Ibid* at § 1109.
[863] *PIPEDA*, *supra* note 643 at Schedule 1.

this can be accomplished by referring to fundamental rights and freedoms in the purpose section of the legislation, using rights-based language in provisions, and adding provisions involving privacy by design, data impact risk assessments, and data fiduciaries.

4.2 Theme 2: Consent and Balancing Rights with Legitimate Interests

The second theme contains selected provisions involving consent and balancing rights with legitimate interests. I list the provisions in the theme, analyze the provisions, and discuss the implications for the new workplace privacy regime.

4.2.1 The Privacy Provisions Examined in Theme 2

As can be seen in the chart below, there are two features of privacy provisions, data protection provisions and employment provisions, which will be discussed in Theme 2:

Table 3: The Privacy Provisions Studied in Chapter 4, Theme 2

Theme	Canada	United States	European Union
2- The consent of individuals and the legitimate interests of organizations	*PIPEDA* *QC Act* *BC PIPA* *PIPEDA Breach Regulations*	*California Labor Code* *California Consumer Privacy Act* *California Civil Code (Customer Records)*	*GDPR*

4.2.2 Analysis of the Privacy Provisions in Theme 2

My goal in this section is to argue that *PIPEDA's* consent-based model is insufficient for dealing with the employment context, especially when it comes to electronic surveillance, and I will demonstrate that it is necessary to find an alternative approach. In addition, I

will show that *PIPEDA* does not appropriately balance the rights of employees with legitimate business interests of employers, and that other jurisdictions use more effective strategies to do so.

I plan to argue for these points in three steps. First, I will suggest that employees are in most cases not in a position to provide, withhold, or revoke consent in situations involving electronic surveillance. Second, I will demonstrate that other jurisdictions have closely examined this issue and have provided some useful insights. Third, I will illustrate how *PIPEDA* does not properly balance the rights of employees with the legitimate business interests of employers, and how other jurisdictions attempt to achieve this goal in more effective ways.

To this end, the first thing to point out is that employees are in most cases not in a position to provide, withhold, or revoke consent in situations involving electronic surveillance. More specifically, the parties in an employment relationship possess inherently unequal bargaining power, and this affects employees' ability to freely provide, withhold, or revoke consent to such monitoring.[864] This is so regardless of unionization status—regardless of whether they are members of a union, employees are still vulnerable and subject to the direction of their employers, and cannot control the nature and extent of the electronic surveillance they experience inside or outside the workplace.[865] Employers are in the dominant position and have many opportunities to abuse their electronic surveillance power at any point during the employment relationship, from the hiring stage through to the post-termination stage.[866] As will be illustrated in Chapter 5, employees can become subject to excessive and/or overly intrusive electronic surveillance that is unilaterally commenced by their employers; the

---

[864] Kirstie Ball, Elizabeth M Daniel & Chris Stride, "Dimensions of Employee Privacy: An Empirical Study" (2012) 25:4 Information Technology & People 376 at 377, online (pdf): *Emerald Group Publishing* <www.emeraldinsight.com> DOI: <10.1108/09593841211278785> [Ball, Daniel & Stride, "Dimensions"]; Shoshana Zuboff, "Smart Machine", *supra* note 700 at 313, 322–327; *Machtinger, supra* note 842 at para 31; *Wallace*, *supra* note 842 at paras 92−93; David Doorey, "Common Law and Regulation", *supra* note 842 at 5−6, 67−75, 111−120; David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 842 at 67, 94−97, 239−241.
[865] *Ibid.*
[866] *Ibid.*

two surveillance scenarios arise in both unionized and nonunionized workplaces, and notwithstanding the degrees of seniority or clout of the employees.[867] This is because, unlike levels of negotiated wages, working conditions, or benefits, where some employees may enjoy higher levels of protection and certain advantages, employers' decisions to use sophisticated electronic surveillance technologies on employees applies to any and all employees, regardless of the employees' status—any employee can become a data subject in the employer's information Panopticon—and exploited through the abuse of electronic surveillance power.[868]

It is therefore concerning that the definition of consent in *PIPEDA* does not specifically discuss an employee's ability to consent and assumes that it can be freely provided, withheld, or revoked. More specifically, section 6.1 of *PIPEDA*[869] states that, for the purposes of clause 4.3 in Schedule 1 of *PIPEDA*[870] dealing with consent, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.[871]

Also, section 14 of the *QC Act*[872] states that consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes, and that consent is valid only for the length of time needed to achieve the purposes for which it was requested. Section 7 of the *BC PIPA*,[873] states that an organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service. In fact, if an organization attempts to obtain consent for collecting, using or disclosing personal information by providing false or misleading information respecting the collection, use or disclosure of the information,

---

[867] See Chapter 5 for further details.
[868] *Supra* note 864.
[869] *PIPEDA, supra* note 643 at s 6.1.
[870] *Ibid* at Schedule 1, cl 4.3.
[871] *PIPEDA, supra* note 643 at s 6.1.
[872] *QC Act, supra* note 646 at s 14.
[873] *BC PIPA, supra* note 645 at s 7.

or using deceptive or misleading practices, then any consent provided in those circumstances is not validly given.[874]

Aspects of consent included in the above definitions cannot practically apply in an employment situation given the asymmetrical power dynamics present in the employment relationship.[875] Since the current definitions insufficiently touch on the vulnerability of employees, it would be advantageous for there to be a provision in *PIPEDA* following the definition of consent that expressly states that employees are not in a position to freely provide, withhold, or revoke consent to the collection, use or disclosure of personal information.

The other reason why novel provisions governing consent are needed is that, in addition to the lack of acknowledgment regarding employees and the ability to provide, withhold, or revoke consent in section 6.1 of *PIPEDA*,[876] there is no recognition of this fact under Principle 3 in clause 4.3 of Schedule 1 of *PIPEDA*[877] dealing with consent. In my view, this is a serious problem. Let me explain.

This legislative oversight can be seen in clause 4.3 of Schedule 1 of *PIPEDA*,[878] where it states:

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. **Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated**. In addition, **organizations that do not have a direct relationship with the**

---

[874] *Ibid.*
[875] *Machtinger*, *supra* note 842 at para 31; *Wallace*, *supra* note 842 at paras 92−93. See also David Doorey, "Common Law and Regulation", *supra* note 842 at 5−6, 67−75, 111−120; David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 842 at 67, 94−97, 239−241.
[876] *PIPEDA*, *supra* note 643 at s 6.1.
[877] *Ibid* at Schedule 1, cl 4.3.
[878] *Ibid*.

> **individual** may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.[879]

What is most striking is that there is a part of the opening phrase of clause 4.3 of Schedule 1 of *PIPEDA*[880] that deals with situations where consent may be impossible or inappropriate, including when the individual is a minor, seriously ill, or mentally incapacitated, and where organizations do not have a direct relationship with the individual as in a charity.[881] However, there is no mention here of employees who are vulnerable parties in an employment relationship and who are not in a position to freely provide, withhold, or revoke consent, even though they are just as vulnerable as minors, seriously ill persons, or mentally incapacitated persons who are not able to consent.[882]

Against this, one might insist that employees are not as vulnerable as minors, or ill or incapacitated individuals. In response, I would return to the fact that it has already been recognized by the Supreme Court of Canada that employees are vulnerable members of society.[883] As explained by Iacobucci J., the power imbalance that is present in the employment relationship "is not limited to the employment contract itself" and "informs all facets of the employment relationship".[884] Iacobucci J. has clarified that employees constitute a vulnerable group: "The vulnerability of employees is underscored by the level of importance which our society attaches to employment".[885] Moreover, Dickson C.J. has also elucidated that employment is one of the most fundamental aspects of life: "A person's employment is an essential component of his or her sense of identity, self-worth and emotional well-being".[886] However, there are no protections in *PIPEDA* that recognize this reality.

---

[879] *Ibid* [emphasis added].
[880] *Ibid*.
[881] *Ibid.*
[882] *Ibid*.
[883] *Machtinger*, *supra* note 842 at para 31; *Wallace*, *supra* note 842 at paras 92−93.
[884] *Wallace*, *supra* note 842 at para 92.
[885] *Ibid* at para 93.
[886] *Reference Re Public Service Employee Relations Act (Alta)*, [1987] 1 SCR 313 at para 95, 1987 CarswellAlta 705 (SCC) [*Alberta Reference*].

Both the opening phrase and the clauses under Principle 3 of Schedule 1 of *PIPEDA*[887] assume that consent is something that can be freely given or refused in the employment context, and do not address the concern regarding employees being vulnerable members of society. There are a number of situations where consent is considered to not be freely given; one situation that would negate one's ability to consent would be where deception is used to obtain the consent.[888] Another situation that would be where organizations try to obtain consent by requiring individuals to provide consent beyond what is required to meet the legitimate purposes.[889]

The same can be said in respect of consent provisions in the *BC PIPA*;[890] the truth is that employees are not able to decline for the purposes of negating implicit consent,[891] or to withdraw their consent.[892] The power imbalances that are present in employment are similarly not addressed sections 7−9 of the *BC PIPA*.[893]

These clauses are not helpful when it comes to the employment relationship. The above discussion suggests that privacy legislation in Canada is based on the prevailing notion that consent is central and that it can be provided, withheld, or revoked by employees. In this sense, the Canadian model uses a control-over-information framework of privacy, and assumes that individuals have the ability to control information and limit access to information about them, presupposing that they are in a position to decide what personal information about themselves can be known by others.[894] Indeed, the Privacy Commissioner of Canada, Daniel Therrien, has stated that his current mandate is to

---

[887] *PIPEDA*, *supra* note 643 at Schedule 1, cl 4.3.
[888] *Ibid* at cl 4.3.5.
[889] *Ibid* at cl 4.3.3.
[890] *BC PIPA*, *supra* note 645 at ss 7−9.
[891] *Ibid* at s 8(3).
[892] *Ibid* at s 9(1), (3).
[893] *Ibid* at ss 7−9.
[894] Ruth Gavison, "Privacy and the Limits of the Law" in David Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 346 at 348; Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (New Jersey: Rowman & Littlefield, 1988) at 3; Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1968) at 7; W A Parent, "A New Definition of Privacy for the Law" (1983) 2 Law and Philosophy 305 at 306; Raymond Wacks, *Personal Information: Privacy in the Law* (Oxford: Clarendon Press, 1989) at 15–16.

increase the control Canadians have over their personal information.[895] Moreover, the Office of the Privacy Commissioner of Canada has recently created guidelines for obtaining meaningful consent,[896] and it becomes clear that there has been an application of principles stemming from clause 4.3 of Schedule 1 of *PIPEDA*,[897] and the same assumption has been made that individuals have the ability to freely provide consent in the first place. For example, one of the guidelines states that it is important to provide individuals with clear options to say "yes" or "no".[898] Individuals cannot be required to consent to the collection, use or disclosure of personal information; they must be given a choice whether to do so.[899]

But in employment relationships, employees do not have a choice when dealing with their employers, because there is an unequal bargaining power between the parties and a large potential for employers to take advantage.[900] When it comes to electronic surveillance technology in the workplace, the potential for employees to be exploited by employers is apparent given the unquestionable asymmetrical power relationships.[901] In particular, employees are typically not permitted to make the same types of choices to protect their privacy compared to regular citizens and consumers, because they are subject to the working practices and environment dictated by their employers; if they want to keep working and making a living, they need to agree to the conditions that are set by their employer.[902] The abuse of the electronic surveillance power to which I refer

---

[895] Office of the Privacy Commissioner of Canada, "The Privacy Commissioner of Canada" (14 December 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/who-we-are/the-privacy-commissioner-of-canada/>.
[896] Office of the Privacy Commissioner of Canada, "Guidelines for Obtaining Meaningful Consent" (24 May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> [Privacy Commissioner, "Meaningful Consent"].
[897] *PIPEDA*, *supra* note 643 at Schedule 1, cl 4.3.
[898] Privacy Commissioner, "Meaningful Consent", *supra* note 896.
[899] *Ibid.*
[900] *Machtinger*, *supra* note 842 at para 31; *Wallace*, *supra* note 842 at paras 92−93. See also David Doorey, "Common Law and Regulation", *supra* note 842 at 5−6, 67−75, 111−120; David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 842 at 67, 94−97, 239−241.
[901] Graham Sewell, James R Barker & Daniel Nyberg, "Working under Intensive Surveillance: When Does 'Measuring Everything That Moves' Become Intolerable?" (2011) 65:2 Human Relations 189 at 207, online (pdf): *SAGE Journals* <hum.sagepub.com> DOI: <10.1177/0018726711428958>.
[902] Ball, Daniel & Stride, "Dimensions", *supra* note 864 at 377.

can be seen when examining the effects on employees who experience an increased sense of vulnerability, powerlessness, and a loss of trust in their employer.[903]

To this point I have shown how employees are in most cases not in a position to provide, withhold, or revoke consent in situations involving electronic surveillance. What I would like to do now is argue that, although there are no provisions in *PIPEDA* dealing with the ability of employees to provide, withhold, or revoke consent, the European Union appears to provide some significant insights in this regard.

More specially, Article 4(11) of the *GDPR*[904] defines consent as any freely given, specific, informed and unambiguous indication of data subjects' wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data about them. Also, Article 7(4) of the *GDPR*[905] sets out the conditions for consent, and it appears to tackle the problem of freely providing consent in power relationships:

> When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[906]

The Article 29 Working Party[907] has stated that this provision aiming to determine whether consent has been freely given plays an important role, because it takes on the situation of bundling consent with the acceptance of terms or conditions, or tying the provision of a contract to a request for consent to process personal data that is not necessary for the performance of the contract, and considers this to be "highly

---

[903] Shoshana Zuboff, "Smart Machine", *supra* note 700 at 344; Peter Jeffrey Holland, Brian Cooper & Rob Hecker, "Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type" (2014) 44:1 Personnel Review 161 at 161, online (pdf): *Emerald Insight* <www.emeraldinsight.com> DOI: <10.1108/PR-11-2013-0211>.
[904] *GDPR*, *supra* note 655 at art 4(11).
[905] *Ibid* at art 7(4).
[906] *Ibid.*
[907] Prior to the enactment of the *GDPR*, the Article 29 Working Party was an advisory body made up of representatives from the data protection authorities of each EU member state, the EU Commission, and the European Data Protection Supervisor. Upon enactment of the *GDPR* on May 25, 2018, the European Data Protection Board replaced it and is governed by Articles 68–76 of the *GDPR*. See European Commission, "Article 29 working party archives 1997–2016" (2020), online: *European Commission* <https://ec.europa.eu/justice/article-29/documentation/index_en.htm>.

undesirable".[908] Any consent provided in this situation is presumed to not be freely given.[909] The purpose of Article 7(4) of the *GDPR*[910] is to ensure that any unnecessary processing is not disguised or bundled with the performance of a contract.[911] This is especially the case when there is a clear imbalance of power between the data subject and the controller.[912]

The Article 29 Working Party has confirmed that an imbalance of power is present in the employment context, and has concluded that for that reason it is unlikely that an employee will be able to withhold consent to data processing without experiencing the fear or real risk of detrimental effects as a result of the refusal.[913] And it is just as unlikely that an employee would be able to respond freely to a request for consent from an employer to activate monitoring systems in the workplace without feeling any pressure to consent.[914] The concept of "free" implies a real choice and consent is not considered to be free if the employee is unable to refuse or withdraw consent without detriment.[915] In my view, the above discussion helps to illustrate why it is problematic to assume that employees, who are the weaker party in the power relationship, can always freely provide, withhold, or revoke consent.

What the preceding discussion suggests is that, when it comes to the electronic surveillance by employers, employees feel real pressures to provide consent; likewise, they cannot realistically withhold or revoke consent without experiencing the fear or real risk of detrimental effects as a result of a refusal. When employees face consequences to

---

[908] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679, WP 259" (28 November 2017) at 9, online (pdf): *European Commission* <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> [Working Party, "Consent Guidelines"].
[909] *Ibid.*
[910] *GDPR*, *supra* note 655 at art 7(4).
[911] Working Party, "Consent Guidelines", *supra* note 908 at 9.
[912] *Ibid* at 7–8.
[913] *Ibid* at 8.
[914] *Ibid.*
[915] *Ibid* at 6. See also Article 29 Data Protection Working Party, "Opinion 8/2001 on the Processing of Personal Data in the Employment Context, WP 48" (13 September 2001) at 21, online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf> [Working Party, "8/2001"].

the point where they cannot genuinely provide an answer to their employers, consent is not considered to be freely provided, withheld, or revoked.

This is concerning, given that employees are more frequently becoming the subjects of electronic surveillance in the workplace using a range of technologies from computer and telephone logging, to CCTV, to mobility tracking, to electronic recruitment.[916] A significant contributor of the increase in employee monitoring is the Internet, and the truth is that it is not uncommon for companies to monitor worker communications and on-the-job activities.[917] If the supervisor is the overseer and the employers are the overseen who attempt to avoid the manager's gaze,[918] then it should not be surprising that both recent technological developments and modern management culture have together magnified the incidence of individual monitoring to the point where electronic surveillance in the workplace may be considered normal and taken for granted.[919]

All the same, it is important to keep in mind that employer-employee relations need to be afforded sufficient flexibility in light of the unique labour relations environment. To address this concern, Article 88 of the *GDPR*[920] allows Member States, by law or by collective agreements, to provide for more specific rules to ensure the rights and freedoms regarding the processing of employees' personal data in the employment context relating to all aspects of the employment relationship; there is an attempt in the European Union to force the parties to include "suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place".[921] This novel strategy can be translated into Canadian workplaces by allowing for the flexibility of the parties to jointly create further specific rules concerning electronic surveillance, while still ensuring that

---

[916] Kirstie Ball, "An Overview", *supra* note 772 at 87.
[917] *Ibid.*
[918] *Ibid;* Sewell, Barker & Nyberg, *supra* note 901 at 192–194.
[919] Kirstie Ball, "An Overview", *supra* note 772 at 87.
[920] *GDPR*, *supra* note 655 at art 88.
[921] *Ibid.*

there is not an abuse of surveillance power by stipulating that employers are required to ensure that adequate safeguards are in place for employees to prevent the use of excessive or overly intrusive electronic surveillance.[922]

However, keeping in mind the inherent unequal bargaining power between the parties and the discussion regarding consent above, this provision would be adapted and practically used in the Canadian employment context in only rare situations. Hence, I would endorse this option only as an exception to the main point that employees are not typically in a position to freely provide, withhold, or revoke consent in situations involving electronic surveillance.[923] When it comes to jointly creating these rules that pertain to electronic surveillance in the workplace, I believe that more egalitarian interactions between the parties allowing for free consent of employees are uncommon for a few reasons. Firstly, the rate of unionization in Canada continues to decline: according to Statistics Canada, overall unionization rates have fallen considerably since 1981, where the percentage of men aged 17 to 64 who belonged to unions dropped from 42 percent in 1981 to 26 percent in 2018.[924] It is also important to keep in mind that unionization rates in the public sector are four times higher than those in the private sector;[925] this suggests that there may be fewer opportunities for private sector employees to achieve a fair balance with their employers regarding electronic surveillance. Secondly, even if there is a union present or a high-level nonunionized employee with more bargaining power, this does not necessarily mean that electronic surveillance concerns will be the subject of collective bargaining or negotiations; in many cases, the focus of both contract negotiations and collective bargaining is typically on higher wages, better working conditions, and other benefits such as pensions or seniority-based benefits

---

[922] *Ibid.*
[923] One example of a rare exception could be a situation where a particularly powerful union advocates for the privacy of its members regarding certain issues involving electronic surveillance in the workplace during more egalitarian collective bargaining sessions. This process would entail incorporating safeguards and other measures to protect the dignity, and prevent the exploitation of, employees in the bargaining unit.
[924] René Morissette, "Changing Characteristics of Canadian Jobs, 1981 to 2018" (30 November 2018) at 1, online (pdf): *Statistics Canada: Economic Insights* <https://www150.statcan.gc.ca/n1/en/pub/11-626-x/11-626-x2018086-eng.pdf?st=GTmudv2A>. That said, there was little change to the unionization rate of women in that age group.
[925] David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 842 at 74−76.

involving access to training and protection from layoffs,[926] to the point where the issue of protection from unreasonable electronic surveillance may often be overlooked. Thirdly, even collective bargaining in unionized workplaces may not necessarily lead to a consensus on the issue of electronic surveillance in the workplace, depending on the power dynamics at play between the particular union and employer; it may be the case that an employer has considerably more power than a union during a collective bargaining session (the bargaining power may not necessarily be even),[927] and can more effortlessly dominate and choose to not include any further protections in a collective agreement or policy. Along the same lines, protections in workplace documents such as policies and procedures regarding electronic surveillance vary substantially among workplaces,[928] and this could be due to the various levels of power employers have relative to each other. Fourthly, it is not necessarily the case that a negotiated contract or a bargained collective agreement or policy actually prevents an employer from conducting unreasonable electronic surveillance. By way of illustration, Chapter 5 discusses cases where employers unilaterally commence excessive and/or overly intrusive electronic surveillance of both unionized and nonunionized employees, some being long-term employees with seniority and more influence, during an employment relationship with agreements, rules or policies in place.[929] Since even in the most ideal employment situations employees are still vulnerable and subject to the direction of their employers, employees are often not in a position to control the nature and extent of employers' electronic surveillance to which they are subjected by relying on consent as an option, agreeing to certain arrangements on electronic surveillance, and ensuring that there are adequate safeguards in place in the workplace to respect employees' dignity.[930]

Let me pause to recap my argument to this point. I first explained why, in most cases, employees are not in a position to provide, withhold, or revoke consent in situations

---

[926] *Ibid* at 94−95.
[927] *Ibid* at 143−144.
[928] Kirstie Ball, "An Overview", *supra* note 772 at 92.
[929] See Chapter 5 for examples of such cases.
[930] Ball & Daniel, "Dimensions", *supra* note 864 at 377; Shoshana Zuboff, "Smart Machine", *supra* note 700 at 313, 324–327; *Machtinger, supra* note 842 at para 31; *Wallace, supra* note 842 at paras 92−93. See also David Doorey, "Common Law and Regulation", *supra* note 842 at 5−6, 67−75, 111−120; David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 842 at 67, 94−97, 239−241.

involving electronic surveillance; I then demonstrated that other jurisdictions have provided useful insights into this matter. The third thing that I will do is argue that *PIPEDA* is not particularly good at balancing the interests of employers and employees, and as a consequence, that there is a skewed set of legislative provisions where the legitimate business interests of employers are ultimately given more attention compared to the privacy interests of employees. This situation can lead to an exacerbation of power imbalances that are inherently present in the employment relationship. Fortunately, there are more useful methods used in the other jurisdictions and I will examine them after noting the problems with *PIPEDA*.

To be clear, I am not suggesting that employers should never be able to collect, use and disclose employees' personal information or that there should be no protections in place when organizations attempt to meet their legitimate business interests such as protecting the data of their clients and customers. Rather, I am suggesting that the amount and quality of *PIPEDA* provisions are currently asymmetrical and in favour of employers relative to employees, preventing a healthy balance of interests.

There are five problematic issues that illustrate the one-sided nature of *PIPEDA's* provisions.

The first problematic issue is that there is a specific provision that allows employers to enjoy what appears to be a substantial amount of power to collect, use and disclose personal the information of employees without consent; if relied upon in situations involving electronic surveillance, there could be a serious abuse of surveillance power. Section 7.3 of *PIPEDA*[931] has two parts: it permits employers to collect, use and disclose personal information without the consent of the employee if: (1) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the employer and the employee; and (2) the employer has informed the individual that the personal information will be or may be collected, used or disclosed for

[931] *PIPEDA*, *supra* note 643 at s 7.3.

those purposes. *PIPEDA* would be improved if this provision[932] were removed. Regarding the first part, there is a lack of clarity since there is no definition of what is, "necessary to establish, manage or terminate an employment relationship";[933] for the purposes of understanding how personal information of employees are to be collected, used and disclosed without consent. This is a considerable weakness, since there is no explanation whatsoever in the definitions in section 7.1 of *PIPEDA*[934] or in anywhere in section 7.3 of *PIPEDA*[935] that provides any guidance as to the boundaries within which employers can operate in this regard. And the second part of section 7.3 of *PIPEDA*[936] uses the phrase "has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes",[937] proceeding as though it is appropriate in the employment context. Moreover, the definition of "personal information" in section 2(1) of *PIPEDA*[938] is quite wide, including several items that could fall under the category of "information about an identifiable individual".[939] This weak requirement to inform amounts to an employer letting the employees know that there will or may soon be a privacy violation, and there is typically nothing that the employees can do about it because of their position in the relationship. Of the jurisdictions studied in this dissertation, this provision is unique to Canada (for instance, similar language is also found in other Canadian jurisdictions such as in the *BC PIPA*).[940] These were the comments of the then Privacy Commissioner of Canada regarding British Columbia's Bill 38, *Personal Information Protection Act*[941] in 2003, before sections 7.1−7.4 of *PIPEDA*[942] were enacted through the *Digital Privacy Act*:[943]

> Third, the Bill is clearly inferior to the PIPED Act with regard to privacy rights in employment. Sections 13, 16 and 19 specifically allow the

---

[932] *Ibid*.
[933] *Ibid* at s 7.3(a).
[934] *Ibid* at s 7.1.
[935] *Ibid* at s 7.3.
[936] *Ibid* at s 7.3.
[937] *Ibid* at s 7.3(b).
[938] *Ibid* at s 2(1).
[939] *Ibid*.
[940] *BC PIPA*, *supra* note 645 at ss 13, 16, 19.
[941] Bill 38, *Personal Information Protection Act*, 4th Sess, 37th Leg, British Columbia, 2003 (assented to October 23, 2003), SBC 2003, c 63.
[942] *PIPEDA*, *supra* note 643 at ss 7.1−7.4.
[943] *Digital Privacy Act*, SC 2015, c 32 [*Digital Privacy Act*].

> collection, use and disclosure of employee personal information without consent. This completely deprives an employee, or a prospective employee, of any control over his or her information.
>
> Although the Bill requires that the collection, use or disclosure of employee personal information be reasonable for the purposes of establishing, managing or terminating an employment relationship, this is a weak test that would not protect employees or prospective employees concerned about their privacy. An employer could argue that almost any intrusion on employee privacy is "reasonable" in the sense that it is potentially helpful for establishing, managing or terminating an employment relationship.
>
> The employee could complain after the fact that this intrusion was not reasonable, but the information would have already been collected and disclosed. Once privacy has been violated, it cannot be unviolated. The damage has been done.[944]

The second problematic issue is that there is an even greater potential for employees to be exploited through the abuse of electronic surveillance power with section 7.4 of *PIPEDA*.[945] It allows organizations to use and disclose employees' personal information for purposes other than those for which the information was collected in any of the circumstances set out in section 7.3 of *PIPEDA*[946] —all without consent and without any stipulations on what the phrase, "for purposes other than those for which it was collected in any of the circumstances set out in" means.[947] Surely, this provision flies in the face of fairness; it is difficult to see how the dignity of employees has been considered at all.[948] The reference to section 7.3 of *PIPEDA*[949] in section 7.4 of *PIPEDA*[950] needs to be removed. In regards to establishing, managing, or terminating an employment relationship,[951] it is unacceptable to create a provision that enables this type of use or disclosure without consent of employees and without any set boundaries within which

---

[944] Office of the Privacy Commissioner of Canada, "Report to Parliament Concerning Substantially Similar Provincial Legislation" (June 2003) at 6, online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/2360/leg-rp_030611_e.pdf>.
[945] *PIPEDA, supra* note 643 at s 7.4.
[946] *Ibid* at s 7.3.
[947] *Ibid* at s 7.4.
[948] Hicks, *supra* note 702 at 16–17.
[949] *PIPEDA, supra* note 643 at s 7.3.
[950] *Ibid* at s 7.4.
[951] *Ibid* at s 7.3.

employers are to operate, relying on mysterious other purposes—there must be protection of employees' dignity and self-respect.[952]

The third problematic issue is that there is further potential for employers to abuse electronic surveillance power by relying on section 7(1)(b) of *PIPEDA*,[953] where they may collect personal information without the knowledge or consent of employees if "it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province".[954] In line with the above discussions regarding "collection" in Theme 1, I suggest that "collection" is insufficient for addressing situations involving electronic surveillance in employment, especially if it is performed without knowledge or consent and constitutes excessive or overly intrusive surveillance that is covert in nature.[955] Indeed, the Office of the Privacy Commissioner of Canada has pointed out that covert video surveillance is an, "extremely privacy-invasive form of technology".[956] In fact, given the nature of the technology such as the ability to gather extraneous information and make judgements about the subject that have nothing to do with the purpose, covert video surveillance should be considered, "only in the most limited cases".[957] Thus, my concerns with section 7(1)(b) of *PIPEDA*[958] are confirmed.

The fourth problematic issue is that there appear to be some hidden dangers with sections 7(1)(b.2), 7(2)(b.2), and 7(3)(e.2) of *PIPEDA*,[959] specifically mentioning information that is produced by individuals in the course of their employment; these provisions state that employers can collect, use or disclose this information without knowledge or consent if

---

[952] *Alberta Reference*, *supra* note 886 at para 95.
[953] *PIPEDA*, *supra* note 643 at s 7(1)(b).
[954] *Ibid.* This could lead to a situation that involves section 7(2)(a) of *PIPEDA*, where personal information is used without knowledge or consent if "in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention".
[955] Kirstie Ball, "An Overview", *supra* note 772 at 92.
[956] Privacy Commissioner, "Video Surveillance", *supra* note 672.
[957] *Ibid.*
[958] *PIPEDA*, *supra* note 643 at s 7(1)(b).
[959] *Ibid* at ss 7(1)(b.2), 7(2)(b.2), 7(3)(e.2).

the collection, use or disclosure is consistent with the purposes for which the information was produced. While these provisions seem less troubling in that they deal with producing a work product and meet legitimate interests of employers to collect, use and disclose information regarding that work output, there is a potential for the abuse of surveillance power—especially since the collection, use or disclosure is permitted without knowledge or consent. What is more, section 7(4) of *PIPEDA*[960] sets the stage for the unlimited abuse of surveillance power by allowing for the use of personal information without consent for purposes other than those for which it was collected in any of the circumstances that are set out in section 7(2)—including section 7(2)(b.2);[961] likewise, section 7(5) of *PIPEDA*[962] enables a situation where there can be a disclosure of personal information without consent for purposes other than those for which it was collected in any of the circumstances in section 7(3)(a) to (h.1)—this includes section 7(3)(e.2).[963] As noted above, it is not clear what is captured with the broad phrase, "for purposes other than those for which it was collected in any of the circumstances set out in",[964] and this is concerning. In particular, the ability to allow for other purposes negates the requirement of consistency with the purposes for which the information was produced, and this could lead to a serious abuse of surveillance power.

The fifth problematic issue is that *PIPEDA* contains several provisions that allow employers to protect their legitimate business interests such as protecting the data of their clients and customers. While this is not problematic in itself, what makes it concerning is that employees are simply not provided with protections that are reciprocal in nature and that protect their interests with equivalent amounts of detail. In addition to the sections mentioned above,[965] it is important to note that section 10.1 of *PIPEDA*[966] sets out several requirements that require proper notification to the Privacy Commissioner of Canada in

---

[960] *Ibid* at s 7(4).
[961] *Ibid* at s 7(2).
[962] *Ibid* at s 7(5).
[963] *Ibid* at s 7(3).
[964] *Ibid* at s 7(4)−(5).
[965] *Ibid* at ss 7.1−7.4, 7(1)(b), 7(1)(b.2), 7(2)(b.2), 7(3)(e.2), 7(4), 7(5).
[966] *Ibid* at s 10.1.

cases of breaches. More specifically, pursuant to section 10.1(1) of *PIPEDA*,[967] organizations must report to the Privacy Commissioner of Canada any breach of security safeguards involving personal information under their control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. "Risk of significant harm" is defined in section 10.1(7) of *PIPEDA*[968] as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. When deciding whether there is significant harm, section 10.1(8) of *PIPEDA*[969] provides three factors to consider: the sensitivity of the personal information involved in the breach; the probability that the personal information has been, is being or will be misused; and any other prescribed factor. Sections 10.1(2) to 10.1(6) of *PIPEDA*[970] contain several reporting requirements involving the reporting as soon as feasible, notifications to individuals, contents of the notification, form and manner, and time limits for giving notification. Moreover, sections 10.2(1) to 10.2(2) of *PIPEDA*[971] state that organizations must notify any other organizations and also government institutions as soon as feasible if it can reduce the risk of harm, or if prescribed conditions are met. Section 10.3 of *PIPEDA*[972] also contains record-keeping requirements. What is more, sections 2 to 6 of the *PIPEDA Breach Regulations*[973] have even more requirements concerning the report to the Privacy Commissioner of Canada, notification to affected individuals, and record-keeping. One example involves the direct and indirect ways to notify the affected individuals of a breach.[974] Another example involves section 2(1) of the *PIPEDA Breach Regulations*,[975] which requires reports of a breach of security safeguards to be in writing and to contain several pieces of information, some of which include: a description of the circumstances

---

[967] *Ibid* at s 10.1(1).
[968] *Ibid* at s 10.1(7).
[969] *Ibid* at s 10.1(8).
[970] *Ibid* at s 10.1(2)−(6).
[971] *Ibid* at s 10.2(1)−(2).
[972] *Ibid* at s 10.3. There are significant fines associated with noncompliance with sections 10.1−10.3, as seen in section 28 of *PIPEDA*.
[973] *PIPEDA Breach Regulations*, *supra* note 644 at ss 2–6.
[974] *Ibid* at ss 4–5.
[975] *Ibid* at s 2(1).

of the breach and, if known, the cause; the day, period or approximate period during which the breach occurred; a description of the personal information that is the subject of the breach; the number or approximate number of individuals affected by the breach; the steps taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm; the steps that the organization has taken or intends to take to notify affected individuals of the breach; and the name and contact information of a person who can answer questions about the breach.

Therefore, it becomes clear that *PIPEDA* provides an uneven distribution of protections to employers and employees. This is so, notwithstanding a provision that appears to provide some job protection to employees in section 27.1(1) of *PIPEDA*,[976] which prohibits employers from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee, or denying an employee a benefit of employment, because the employee acts in good faith and on the basis of reasonable belief, and discloses to the Privacy Commissioner of Canada that the employer or any other person has contravened or intends to contravene a provision of Division 1 (protection of personal information) or Division 1.1 (breaches of security safeguards).[977] The same is true in cases where employees refuse to violate these Divisions or experience mistreatment because they comply with *PIPEDA*.[978] I would like to suggest that this protective provision is insufficient to provide an adequate balance of the interests, and more is required to achieve an equally balanced set of protections for the parties.

If *PIPEDA* provides an unequal distribution of protections in favour of meeting the legitimate interests of employers, it might be said that provisions in California provide a more balanced approach by creating privacy protections on one hand, such as sections 1798.120 and 1798.125(a)(1) the *California Consumer Privacy Act*[979] or section 980 of the *California Labor Code*,[980] while simultaneously providing explicit provisions that

---

[976] *PIPEDA*, *supra* note 643 at s 27.1(1).
[977] *Ibid* at ss 5−10.3.
[978] *Ibid*. There are significant fines associated with noncompliance with section 27.1(1), as seen in section 28 of *PIPEDA*.
[979] *California Consumer Privacy Act*, *supra* note 649 at §§ 1798.120, 1798.125(a)(1).
[980] *California Labor Code*, *supra* note 650 at § 980.

protect the legitimate interests of organizations on the other hand, such as in sections 1798.145(a) and (b) the *California Consumer Privacy Act*[981] and extensive breach notification provisions in its *California Civil Code (Customer Records).*[982] Some provisions are examples applying to the consumer context, but we see that they illustrate how protections can be provided to the parties in a way that is more equally balanced.

For example, California provides employees with specific protective legislative measures in its employment provisions by enacting a provision that prevents employers from forcing employees to provide usernames and passwords for their social media accounts.[983] Section 980 of the *California Labor Code*[984] is technologically responsive in that it deals with practical concerns of job applicants and current employees who feel pressured to provide this information to employers.[985] "Social media" is broadly defined as an electronic service or account, or electronic content, some of which include videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet website profiles or locations.[986] Section 980(b) of the *California Labor Code*[987] states that employers are not allowed to require or request employees or job applicants to: disclose a username or password for the purpose of accessing personal social media; access personal social media in the presence of the employer; or divulge any personal social media. And section 980(e) of the *California Labor Code,*[988] prohibits employers from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against employees or job applicants for not complying with requests that violates the rules in section 980. Yet, employers' interests are taken into account; employers can still request that an employee divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related

---

[981] *California Consumer Privacy Act*, *supra* note 649 at § 1798.145(a)−(b).
[982] *California Civil Code (Customer Records)*, *supra* note 651.
[983] *California Labor Code*, *supra* note 650 at § 980.
[984] *Ibid.*
[985] Bennett et al, "Transparent Lives", *supra* note 689 at 168, 170–171, 179.
[986] *California Labor Code, supra* note 650 at § 980(a).
[987] *Ibid* at § 980(b).
[988] *Ibid* at § 980(e).

proceeding.[989] Similarly, employers are also allowed to require or request that an employee disclose a username, password, or other method to access an employer-issued electronic device.[990] In my view, section 980 of the *California Labor Code,*[991] is a forward-thinking law and addresses valid concerns about intrusions into the personal lives of employees and their coveted social media data; simultaneously, it provides a balance and allows employers to meet their legitimate business interests.

While there are protections in place to prevent the abuse of surveillance power and exploitation of employees' personal data, California also has provisions to protect the legitimate business interests of employers such as protecting client data. For instance, in section 1798.81.5 (a) and (b) of the *California Civil Code (Customer Records),*[992] encourages businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information; in fact, businesses that own, license, or maintain personal information about a California resident are required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Section 1798.82 (g) of the *California Civil Code (Customer Records)*[993]defines "breach of the security of the system" as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Section 1798.82 (a) of the *California Civil Code (Customer Records),*[994] requires businesses in California that own or license computerized data including personal information to disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California: whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; or whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption

---

[989] *Ibid* at § 980(c).
[990] *Ibid* at § 980(d).
[991] *Ibid* at § 980.
[992] *California Civil Code (Customer Records), supra* note 651 at § 1798.81.5 (a)−(b).
[993] *Ibid* at § 1798.82 (g).
[994] *Ibid* at § 1798.82 (a).

key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. Further, section 1798.82 (a) of the *California Civil Code (Customer Records),*[995] requires that these businesses make the disclosure in the most expedient time possible and without unreasonable delay. Section 1798.82 (b) of the *California Civil Code (Customer Records),*[996] states that, in the event of a security breach, businesses must notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. There are several requirements regarding the format of the notification, as set out in 1798.82 (d) of the *California Civil Code (Customer Records).*[997]

A more attractive approach can be found in Article 6(1) of the *GDPR*[998] on the lawfulness of processing of personal data, where several factors are considered, and processing is considered to be lawful only if at least one of the following applies:

> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

---

[995] *Ibid.*
[996] *Ibid* at § 1798.82 (b).
[997] *Ibid* at § 1798.82 (d). See also balanced provisions set out in *California Consumer Privacy Act, supra* note 649 at §§ 1798.120, 1798.145(a)–(b).
[998] *GDPR, supra* note 655 at art 6(1).

> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[999]

A fair balancing is more likely to occur using this novel approach. In the employment relationship, since consent is in most cases not possible due to the unequal bargaining power and consequent lack of ability to freely consent, other factors can be considered such as section 6(1)(f) of the *GDPR*,[1000] requiring a balance between the legitimate interests of the controller or third party and the interests or fundamental rights and freedoms of data subjects. In my view, this provision is well-structured. It also takes into account other possibilities, such as the need to protect the vital interests of the employee[1001] or comply with a legal obligation,[1002] while still leaving open the possibility of consent in the rare circumstances where consent can be freely provided, withheld, or revoked.[1003] While Articles 33 and 34 of the *GDPR*[1004] also set out breach notification requirements that are similar to sections 10.1−10.3 of *PIPEDA*,[1005] sections 2 to 6 of the *PIPEDA Breach Regulations*,[1006] and sections 1798.81.5 and 1798.82 of the *California Civil Code (Customer Records)*,[1007] we see that the novel balancing approach set out in section 6(1) of the *GDPR*,[1008] is beneficial because it uniquely and efficiently takes into consideration the crux of the data protection issue regarding balancing of rights with legitimate interests in the employment context.

The Article 29 Working Party clarifies issues related to consent and legitimate interests, and explains how one would go about conducting what I will call an "assessment of proportionality", in line with section 6(1) of the *GDPR*:[1009]

---

[999] *Ibid.*
[1000] *Ibid* at art 6(1)(f).
[1001] *Ibid* at art 6(1)(d).
[1002] *Ibid* at art 6(1)(c).
[1003] *Ibid* at art 6(1)(a).
[1004] *Ibid* at arts 33−34.
[1005] *PIPEDA, supra* note 643 at ss 10.1−10.3.
[1006] *PIPEDA Breach Regulations, supra* note 644 at ss 2–6.
[1007] *California Civil Code (Customer Records), supra* note 651 at §§ 1798.81.5 (a)−(b), 1798.82 (a)−(g).
[1008] *GDPR, supra* note 655 at art 6(1).
[1009] *Ibid*.

> Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.
>
> The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary.[1010]

To this end, to address the above problematic issues involving the asymmetry of *PIPEDA* protections in the employment context, I would like to suggest that many legitimate employment-related concerns dealing with electronic surveillance could be more effectively addressed as proposed above by balancing privacy rights of employees with legitimate business interests of employers using an assessment of proportionality. This is especially the case when dealing with situations involving electronic surveillance, for instance, with the above example regarding section 7(1)(b) of *PIPEDA.*[1011]

However in my view, the word "lawful" leaves me with an impression that the decision is fixed on a single analysis, where processing is considered to be either lawful or not; given the fluid and multi-dimensional nature of electronic surveillance, I would like to suggest that, instead of asking whether the electronic surveillance is lawful as in section 6(1) of the *GDPR,*[1012] more appropriate questions to ask include whether an employer may conduct the electronic surveillance, and whether the employer may continue to conduct

---

[1010] Article 29 Data Protection Working Party, "Opinion 2/2017 on the Data Processing at Work, WP 249" (8 June 2017) at 21, online (pdf): *European Commission* <https://ec.europa.eu> [Working Party, "2/2017"]. See also Recital 4 for further information regarding balancing rights and the principle of proportionality at Information Commissioner's Office, "GDPR recitals and articles" (2016), online: *Information Commissioner's Office* <https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf>.

[1011] *PIPEDA, supra* note 643 at s 7(1)(b). While I propose completely removing section 7.3 and references to 7.3 in 7.4 of *PIPEDA*, there are several opportunities to use the assessment of proportionality instead of having rigid rules that are skewed in favour of employers, as mentioned above.

[1012] *GDPR, supra* note 655 at art 6(1).

the electronic surveillance upon further assessments of proportionality to ensure that the electronic surveillance remains necessary and proportionate at the current levels, or whether any aspects of the electronic surveillance have become excessive and/or overly intrusive and it is time to modify or cease the unreasonable electronic surveillance.

Employers have legitimate business interests that must be recognized during the assessment of proportionality. More specifically, there are three main reasons why employers might want to monitor employees: to maintain productivity and monitor resource use by employees; to protect corporate interests and trade secrets (including minimizing risks of defamation, sabotage, data theft, and hacking); and to protect the company from legal liability.[1013] Thus, it is important to appreciate that employee monitoring can serve as a significant risk management tool for employers to limit costs and risks, protect value, and maintain quality.[1014]

All the same, there are significant threats to the employment relationship that cannot be ignored.[1015] There are challenges when the electronic surveillance goes beyond what is considered necessary and when the monitoring negatively affects existing levels of control, autonomy, and trust.[1016] One consequence of excessive or overly intrusive monitoring is a fear among employees that their employers may disclose personal information to unknown third parties.[1017] Another consequence is that it may cause some employees to experience physical symptoms such as pain and psychological symptoms such as low self-esteem, anxiety, and depression.[1018] A further disturbing consequence is that there is a danger of anticipatory conformity, where employees behave in docile and accepting ways; as a result, employees become less committed and less motivated.[1019]

[1013] Kirstie Ball, "An Overview", *supra* note 772 at 92.
[1014] *Ibid.*
[1015] *Ibid* at 98–99.
[1016] *Ibid* at 89.
[1017] *Ibid.*
[1018] Kirstie S Ball & Stephen T Margulis, "Electronic Monitoring and Surveillance in Call Centers: A Framework for Investigation" (2011) 26:2 New Technology, Work and Employment 113 at 116–117, online (pdf): *Wiley Online Library* <https://onlinelibrary.wiley.com/journal/1468005X> [Ball & Margulis, "Framework"].
[1019] Kirstie Ball, "An Overview", *supra* note 772 at 93–94.

Some employees even bend and manipulate company rules or sabotage the workplace.[1020] Therefore, a fair balance must be achieved between the parties to minimize the negative effects of the abuse of surveillance power and ensure that underlying trust is not destroyed—this is what is required to prevent employees from being excessively controlled and exploited.[1021]

In this part, I have argued that *PIPEDA's* consent-based model was insufficient for dealing with the employment context, especially in situations involving electronic surveillance, and also that *PIPEDA* did not effectively balance the rights of employees with legitimate business interests of employers. I did this by showing that employees were often not in a position to provide, withhold, or revoke consent in situations involving electronic surveillance, and examining how other jurisdictions tackled this issue. I also explained how *PIPEDA* did not properly balance the rights of employees with the legitimate business interests of employers, and how other jurisdictions have done so in more effective ways.

4.2.3 Implications for the New Workplace Privacy Regime

I have argued that Canada's consent-based model of privacy protections is insufficient for dealing with current issues involving relationships characterized by power imbalances, particularly the employment relationship. It certainly does not help to solve the problem of closing the electronic surveillance gap in employment. This is why, in my view, new provisions are required to squarely address these increasingly important issues. That said, given the need to attend to the rare circumstances where parties require the flexibility to create further specific data protection rules that apply in their specific workplaces, it seems to me that new provisions are warranted—attached with extra protections that ensure that adequate safeguards are in place. In addition, I argued that there are critical problems with *PIPEDA* when it comes to its ability to balance the interests of the parties in the employment context. Currently, the provisions are skewed in favour of protecting

---

[1020] *Ibid* at 89.
[1021] Holland, Cooper & Hecker, *supra* note 903 at 163–164; Shoshana Zuboff, "Smart Machine", *supra* note 700 at 313.

the interests of employers, and this creates a situation where employees' data protection concerns of employees are being forgotten. In my view, it is necessary to create more suitable provisions that properly deal with the electronic surveillance of employees in a balanced manner, and this can be achieved by using an assessment of proportionality. There are also several ideas that can be borrowed from other jurisdictions and incorporated into the new workplace privacy regime to protect employees, such as prohibiting employers from forcing employees to provide their social media usernames and passwords.

4.3 Theme 3: Order-Making Powers, Penalties, and Fines

The third theme contains selected provisions involving order-making powers, penalties, and fines. I list the provisions in the theme, analyze the provisions, and discuss the implications for the new workplace privacy regime.

4.3.1 The Privacy Provisions Examined in Theme 3

As can be seen in the chart below, there is one feature of privacy provisions, namely data protection provisions, which will be discussed in Theme 3:

Table 4: The Privacy Provisions Studied in Chapter 4, Theme 3

Theme	Canada	United States	European Union
3- Order-making powers, Penalties, and Fines	*PIPEDA* *BC PIPA* *QC Act*	*California Consumer Privacy Act*	*GDPR*

4.3.2 Analysis of the Privacy Provisions in Theme 3

My goal in this section is to argue that *PIPEDA* does not provide the Privacy Commissioner of Canada with the necessary order-making powers or the ability to impose proportional penalties, especially in regards to electronic surveillance.

I will argue for this conclusion in three steps. First, I will point out that it is not clear why the Privacy Commissioner of Canada does not have order-making powers or the ability to impose meaningful penalties. Second, I will show that provisions in other Canadian and American jurisdictions provide these powers. And third, I will examine the European Union and stress that there are several useful strategies for creating penalties and imposing fines in cases of noncompliance.

It is important to highlight at the outset that it is not clear why the Privacy Commissioner of Canada does not have binding order-making powers or the ability to impose meaningful proportional penalties for non-compliance with *PIPEDA*; unlike Commissioners in other Canadian jurisdictions, the Privacy Commissioner of Canada must go to the Federal Court to obtain a court order.[1022] More specifically, one avenue that the Privacy Commissioner of Canada can take is to enter into a compliance agreement with an organization to ensure the organization's compliance with *PIPEDA*—and when the agreement is not complied with, the Privacy Commissioner of Canada may then apply to the Federal Court for an order requiring the organization to comply with the terms of that agreement.[1023] More specifically, section 17.1(1) of *PIPEDA*[1024] states that compliance agreements are created when the Privacy Commissioner of Canada believes on reasonable grounds that an organization has committed, is about to commit, or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 (protection of personal information) or Division 1.1 (breaches of security safeguards)[1025] or a failure to follow a recommendation set out in Schedule 1 of *PIPEDA*.[1026] Another avenue that the Privacy Commissioner can take is to rely on section 15(a) of *PIPEDA*[1027] and apply to the Federal Court, with the consent of the complainant, for a hearing in respect of any matter that it did not initiate and seek such orders as are necessary to ensure an organization's compliance with *PIPEDA*. The Federal Court

---

[1022] *PIPEDA*, *supra* note 643 at ss 2(1), 14−17.2.
[1023] *Ibid* at ss 17.1−17.2.
[1024] *Ibid* at s 17.1(1).
[1025] *Ibid* at ss 5−10.3.
[1026] *Ibid* at Schedule 1.
[1027] *Ibid* at s 15(a). Matters initiated by complainants are dealt with in section 14. The hearing by the court can be in respect of any matter in respect of which the complaint was made, or that is referred to in the Privacy Commissioner of Canada's report of findings, and that is referred to in certain sections of *PIPEDA*.

would then be able to order an organization to do several things, one of which could include correcting its practices in order to be in compliance with *PIPEDA*.[1028]

If the goal is to provide protections equally to all Canadians in line with the idea that all Canadians are worthy of the same types of privacy protections to preserve their human dignity,[1029] then it is not clear why the consequences for privacy violations would vary throughout the country, and for the most part, be weakest when dealing with *PIPEDA*.

Indeed, in his recent statements discussing the 2018−2019 Annual Report[1030] the Privacy Commissioner of Canada, Daniel Therrien,[1031] stated:

> Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. It is the role of government to give Canadians the assurance that legislation will protect their rights.
>
> Given that privacy is a fundamental human right and a necessary precondition to the exercise of other fundamental rights such as freedom and equality, the starting point should be to give privacy laws a rights-based foundation.
>
> In other words, new privacy laws should reflect fundamental Canadian values…
>
> It is untenable that organizations like Facebook are allowed to reject my office's findings as mere opinions. The law should no longer be drafted as an industry code of suggested best practices, but rather as a set of enforceable rights and obligations.
>
> Third, **we need enforcement mechanisms that offer quick, effective remedies** for people whose privacy rights have been violated, and that help to ensure ongoing compliance by organizations.
>
> This **includes empowering the Privacy Commissioner to make binding orders and impose consequential, but proportional penalties for non-compliance with the law**.

[1028] *PIPEDA*, *supra* note 643 at s 16.
[1029] George Kateb, *Human Dignity* (Cambridge: Harvard University Press, 2011) at 5–9.
[1030] Privacy Commissioner, "2018–2019 Annual Report", *supra* note 810.
[1031] Daniel Therrien was appointed Privacy Commissioner of Canada on June 5, 2014 after three decades serving Canadians as a lawyer with various federal departments where human rights issues were important. Commissioner Therrien's current mandate is to increase the control Canadians have over their personal information. See Office of the Privacy Commissioner of Canada, "The Privacy Commissioner of Canada" (14 December 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/who-we-are/the-privacy-commissioner-of-canada/>.

> As well, my office should be enabled to conduct proactive inspections to ensure organizations are demonstrably accountable for their privacy practices…
>
> Before closing, I want to emphasize that a rights-based law is not an impediment to innovation. To the contrary: good privacy laws are key to promoting trust in both government and commercial activities.
>
> Without that trust, innovation, growth and social acceptance of government programs can be severely affected.[1032]

The Privacy Commissioner of Canada stresses that enforcement mechanisms should result in quick and effective remedies for individuals and broad and ongoing compliance by organizations; true order-making powers and fines would change the dynamics during investigations and lead to quicker resolution for Canadians.[1033] However, these calls have not yet been answered, despite years of the Privacy Commissioner reiterating this point: "For several years, my predecessors and I have been calling for fundamental reform of Canada's privacy laws".[1034] There appears to be a disconnect between what the Privacy Commissioner of Canada believes is required and what is being enacted by Parliament. In my view, it is necessary to move from the soft-resolution approaches of the past to a deterrence approach through the imposition of enforceable rights and duties.[1035] What currently exists is no longer appropriate in today's rapidly evolving technological context, especially given the global nature of the informational economy and organizations' growing tendency to disregard data protection rules.[1036]

I take myself to have shown that it is not clear why the Privacy Commissioner of Canada does not have order-making powers or the ability to impose meaningful penalties. Let me move on to the second thing that I said I would do in this section, namely show how provisions in other Canadian and American jurisdictions provide these powers.

[1032] Office of the Privacy Commissioner of Canada, "Remarks by Privacy Commissioner of Canada regarding his 2018-19 Annual Report to Parliament" (10 December 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20191210/> [emphasis added].
[1033] Privacy Commissioner, "2018–2019 Annual Report", *supra* note 810 at 5.
[1034] *Ibid* at 2.
[1035] Teresa Scassa, "Moving on from the Ombuds Model for Data Protection in Canada" (2019) 17 CJLT 90 at 94−95.
[1036] *Ibid* at 95−97.

With respect to order-making powers, the Information and Privacy Commissioner for British Columbia has several order-making powers, and organizations must comply with these orders.[1037] Section 52(1) to (4) of *BC PIPA*[1038] sets out order-making powers, including: dealing with access requests such as requiring an organization to give access to all or part of a person's personal information or disclosing how personal information has been used; dealing with access refusals such as confirming the decision of the organization or requiring the organization to reconsider its decision; and making other orders such as dealing with fees, confirming a decision not to correct personal information, requiring an organization to stop collecting, using or disclosing personal information, or requiring an organization to destroy personal information that was improperly collected. Moreover, the section 55 of the *QC Act*[1039] more generally states that the Commission d'accès à l'information has all the powers necessary for the exercise of its jurisdiction, and may make any order it considers appropriate to protect the rights of the parties and rule on any issue of fact or law. Not only is it necessary for the Privacy Commissioner of Canada to have these types of order-making powers in *PIPEDA*, but it is also important, at least in my view, to add a power to make an order prohibiting acts of unreasonable electronic surveillance, and an offence relating to acts of unreasonable electronic surveillance. In addition to the existing powers relating to regular investigations, I believe that it is also essential to add an explicit power for the Privacy Commissioner of Canada to proactively inspect, as it sees fit and without the need for an investigation to be taking place, organizations' evidence of compliance to more effectively facilitate its order-making powers and to impose meaningful penalties.

When it comes to penalties, I believe that the Privacy Commissioner of Canada must have the ability to impose proportional fines as well. For example, section 56 of the *BC PIPA*[1040] sets out the offences and penalties, and there are consequences for noncompliance. Individuals who commit an offence can be fined up to $10,000; persons other than an individual can be fined up to $100,000. Likewise, the *QC Act* allows for the

---

[1037] *BC PIPA*, *supra* note 645 at ss 52−53.
[1038] *Ibid* at s 52(1)−(4).
[1039] *QC Act*, *supra* note 646 at s 55.
[1040] *BC PIPA*, *supra* note 645 at s 56.

ability to issue fines for noncompliance.[1041] However, the penal provisions set out a range of fines, depending on the type of offence; typically, fines go up to $10,000, and there is also a feature of adding an additional fine of up to $20,000 for subsequent offences.[1042] It is important to note that there are some fines that are up to $50,000 and up to $100,000 for subsequent offences.[1043] In addition, section 1798.155(b) of the *California Consumer Privacy Act*[1044] similarly sets out the consequences for violations against consumers, businesses, service providers, or other persons that commit a violation are subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.[1045] While this information regarding California applies to the consumer context, we can see that there has been an attempt to provide financial consequences and consider intent, where intentional violations have higher penalties attached to them.[1046] In my view, the fines can be more meaningful if they correspond to the offence based on categories of severity, intention, and continuity of offences. Further, it is my contention that gross profits and size of the business/enterprise are useful factors to list in *PIPEDA* when considering the imposition of fines.

Another essential consideration is the effect of the order. Section 57(1) of the *BC PIPA*[1047] states that where the Commissioner has made an order against an organization and the order has become final as a result of there being no further right of appeal, an individual affected by the order has a cause of action against the organization for damages for actual harm suffered as a result of the breach by the organization of obligations. Likewise, section 58 of the *QC Act*[1048] states that a decision by the Commission d'accès à l'information the Commission becomes executory as a judgment of the Superior Court and has all the effects of such a judgment once filed with the court. And in section 1798.155(b) of the *California Consumer Privacy Act*,[1049] while there is no

---

[1041] *QC Act*, *supra* note 646 at ss 91–93.
[1042] *Ibid.*
[1043] *Ibid.*
[1044] *California Consumer Privacy Act*, *supra* note 649 at § 1798.155(b).
[1045] *Ibid.*
[1046] *Ibid.*
[1047] *BC PIPA*, *supra* note 645 at s 57(1).
[1048] *QC Act*, *supra* note 646 at s 58.
[1049] *California Consumer Privacy Act*, *supra* note 649 at § 1798.155(b).

Privacy Commissioner in this jurisdiction, we can see that the civil penalties must be exclusively assessed and recovered in a civil action. Again, it is my view that the Privacy Commissioner of Canada should be able to have this impact when making orders to prevent unnecessary time delays and hassles—I believe that it is a waste of time and money for everyone involved to have to force the Privacy Commissioner of Canada to go to the Federal Court as with the recent matter involving Facebook, demonstrate with evidence and arguments that an organization did not comply with *PIPEDA* by explaining the findings of its investigation to show that the organization refused to implement the recommendations, and subsequently ask for a declaration that there was a contravention along with several orders to comply with *PIPEDA*.[1050] That is, *PIPEDA* would be improved if the problematic provisions forcing the matter to be resolved by the Federal Court[1051] were removed, and the necessary order-making powers described above were given to the Privacy Commissioner of Canada.

Again, I have demonstrated that it is not clear why the Privacy Commissioner of Canada does not have order-making powers or the ability to impose meaningful fines, and I illustrated that provisions in other Canadian and American jurisdictions provide these powers. The third thing that I will do is show how the European Union goes even further.

[1050] Office of the Privacy Commissioner of Canada, "Privacy Commissioner Files Notice of Application with the Federal Court Against Facebook, Inc" (6 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206/> ; Office of the Privacy Commissioner of Canada, "Notice of Application with the Federal Court Against Facebook, Inc" (6 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/court_p/na_fb_20200206/>; Office of the Privacy Commissioner of Canada, "Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia" (25 April, 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>. See also Daniel Leblanc, "Privacy Watchdog Takes Facebook to Court Over Possible Misuse of Personal Information" (6 February 2020), online: *The Globe and Mail* <https://www.theglobeandmail.com/politics/article-privacy-watchdog-takes-facebook-to-court-over-possible-misuse-of/>; Peter Zimonjic, "Proceedings Launched After Facebook Refused to Implement Commissioner's Recommendations to Protect Privacy" (6 February 2020), online: *CBC News* <https://www.cbc.ca/news/politics/facebook-privacy-commissioner-hearing-1.5454525>.

[1051] *PIPEDA*, *supra* note 643 at ss 14−17.2.

More precisely, when it comes to the order-making powers, Article 58 of the *GDPR*[1052] gives each supervisory authority several investigative, corrective, and authorization and advisory powers. Let me focus on a few examples. Article 58(1)(b) of the *GDPR*[1053] provides each supervisory authority with the power to carry out investigations in the form of data protection audits; also, Article 58(1)(d) of the *GDPR*[1054] provides each supervisory authority with the power to notify the controller or the processor of an alleged infringement of the *GDPR*. What is most interesting is Article 58(2) of the *GDPR*,[1055] which sets out several corrective powers for supervisory authorities, some of which include: issue warnings to controllers or processors regarding likely infringements of the *GDPR*;[1056] issue reprimands where processing operations have infringed the *GDPR*;[1057] order controllers or processors to comply with the data subjects' requests to exercise rights pursuant to the *GDPR*;[1058] order controllers or processors to bring processing operations into compliance with the *GDPR;*[1059] order the controller to communicate a personal data breach to the data subject;[1060] impose a temporary or definitive limitation including a ban on processing;[1061] order the rectification or erasure of personal data or restriction of processing under the *GDPR*;[1062] and impose administrative fines pursuant to Article 83, in addition to, or instead of measures referred to in Article 58(2) the *GDPR*.[1063] These powers are extensive, and I would like to suggest that the Privacy Commissioner of Canada should be equipped with some of these powers as applicable to the Canadian employment context.[1064]

[1052] *GDPR*, *supra*, note 655 at art 58.
[1053] *Ibid* at art 58(1)(b).
[1054] *Ibid* at art 58(1)(d).
[1055] *Ibid* at art 58(2).
[1056] *Ibid* at art 58(2)(a).
[1057] *Ibid* at art 58(2)(b).
[1058] *Ibid* at art 58(2)(c).
[1059] *Ibid* at art 58(2)(d).
[1060] *Ibid* at art 58(2)(e).
[1061] *Ibid* at art 58(2)(f).
[1062] *Ibid* at art 58(2)(g).
[1063] *Ibid* at art 58(2)(i).
[1064] I acknowledge that there are some differences between *PIPEDA* and the *GDPR*. For instance, *PIPEDA* does not list controllers and processors in the same way that the *GDPR* does. See Article 4(7) and 4(8) for the differences (the processor processes personal data on behalf of the controller, and the controller determines the purposes and means of the processing of personal data). Also, the *GDPR* refers to

In terms of fines, Article 83(1) to 83(6) of the *GDPR*[1065] sets out administrative fines and assigns them to two categories of either administrative fines up to €10,000,000, or in the case of an undertaking, up to two percent of the total worldwide annual turnover of the preceding financial year, whichever is higher, or administrative fines up to €20,000,000, or in the case of an undertaking, up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. Also, there are 11 listed factors to consider when imposing the administrative fines, since the fines depend on the circumstances of each case.[1066] Briefly, the factors involve these ideas: (1) nature, severity, and duration of the infringement; (2) the intentional or negligent character of the infringement; (3) any action taken to mitigate the damage suffered by data subjects; (4) the controller/processor's degree of responsibility of the controller considering technical and organizational measures implemented; (5) any relevant previous infringements by the controller/processor; (6) the degree of cooperation with the supervisory authority; (7) the categories of personal data affected by the infringement; (8) how the infringement became known to the supervisory authority (manner of notification of the infringement); (9) compliance with measures previously ordered to be taken; (10) adherence to approved codes of conduct under Article 40, or approved certification mechanisms under Article 42; and (11) any other aggravating or mitigating factors such as financial benefits gained or losses avoided.[1067]

It is important to mention that powers given to supervisory authorities regarding the imposition of administrative fines are taken very seriously. This is in part due to the need to ensure that legal remedies in national courts are effective and have an equivalent effect

---

supervisory authorities, who are independent public authorities which are established by Member States; see Article 4(21). But all the same, I believe that there are some important powers that can be borrowed and given to the Privacy Commissioner of Canada, such as imposing fines.

[1065] *GDPR, supra*, note 655 at art 83(1)−(6).

[1066] *Ibid* at art 83(2).

[1067] *Ibid.*

as the administrative fines imposed by supervisory authorities where a the legal system of a Member State does not provide for administrative fines.[1068]

However, while I agree with many aspects of the European Union's approach to enforcement of orders, in my view the fines are too high and are not appropriate for the Canadian privacy context. This is also my view when considering the fines associated with the Canadian employment context, since maximum penalties are not that high. For instance, the fines set out in Ontario's *Employment Standards Act*[1069]are up to $50,000 for individuals and $100,000 for corporations;[1070] repeated offences carry fines of up to $250,000 for individuals and $500,000 for corporations.[1071] Likewise, the fines set out in Ontario's *Labour Relations Act*[1072]are up to $2,000 for individuals and $25,000 for corporations, trade unions, councils of trade unions or employers' organizations;[1073] continued offences occur for each day the contravention persists, and constitutes a separate offence.[1074] Similarly, fines set out in the *Canada Labour Code*[1075] are up to $10,000 (first offence), $20,000 (second offence), and $50,000 (for each subsequent offence) for those other than corporations;[1076] they are up to $50,000 (first offence), $100,000 (second offence), and 250,000 (for each subsequent offence) for corporations.[1077]

[1068] *Ibid* at arts 58(5)–(6), 83(9). More specifically, Article 58(5) requires Member States to provide by law that its supervisory authority must have the power to bring infringements of the *GDPR* to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings. Article 58(6) gives Member States the power to provide by law additional powers to supervisory authorities. Article 83(9) states that, where the legal system of a Member State does not provide for administrative fines, Article 83 may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities.
[1069] *Employment Standards Act*, 2000, SO 2000, c 41.
[1070] *Ibid* at s 132(a)–(b).
[1071] *Ibid* at s 132(c)
[1072] *Labour Relations Act*, 1995, SO 1995, c 1, Schedule A.
[1073] *Ibid* at s 104(1).
[1074] *Ibid* at s 104(2).
[1075] *Canada Labour Code*, RSC, 1985, c L-2.
[1076] *Ibid* at s 256(1.1)(b).
[1077] *Ibid* at s 256(1.1)(a).

Comparative legal methodologists recommend that it is important to respect the cultural contexts and refrain from mechanically performing legal transplants.[1078] Indeed, it is telling that the fines compared in Canadian data protection and employment are much lower than those imposed in the European Union's *GDPR*; in accordance with the dignity/human rights theoretical approach to privacy, the European Union may be operating with an agenda to proactively protect the dignity of citizens and deter large, wealthy technology companies from misusing their personal data and abusing surveillance power by creating the potential to award very high fines.[1079] Yet, it has been noted in a recent report by the Center for International Governance Innovation (CIGI)[1080] that many of the fines that have been levied so far have posed little threat to cash-rich companies, since most have been relatively minor:

> Although fines were imposed on 91 different companies in GDPR's first year of implementation, most were relatively minor; a single fine accounted for 89 percent of the total €56 million in fines issued. And even this €50 million fine levied against Google is far from the maximum allowable fine of €3.7 billion (which would be four percent of Google's entire global revenue).[1081]

Thus, realistically speaking, the fines have not been as high as one might assume given the structure of the European Union's privacy regime. Still, I believe that the amounts articulated in the *GDPR*[1082] are too high for Canadian private sector organizations, and I would like to suggest that values be set lower so that Canadians will be more willing to accept a new workplace privacy regime.[1083]

That said, for the organizations that take advantage and severely abuse their electronic surveillance power, I would like to suggest that there be an additional offence in *PIPEDA* dealing with mass electronic surveillance for the purposes of manipulating individuals for political, advertising, or other controlling purposes. In this situation, I believe that it

---

[1078] Samuel, *supra* note 656 at 124–134; Van Hoecke, *supra* note 656 at 3−6, 11, 28, 30; Siems, *supra* note 656 at 136−138.
[1079] *GDPR*, *supra*, note 655 at art 83(1)−(6)
[1080] Jeanette Herrle & Jesse Hirsh, "The Peril and Potential of the GDPR" (9 July 2019), online: *CIGI* <https://www.cigionline.org/articles/peril-and-potential-gdpr>.
[1081] *Ibid.*
[1082] *GDPR*, *supra*, note 655 at art 83(1)−(6).
[1083] Geist, *supra* note 794.

would be useful to create higher maximum penalties so that there can be extra leeway for decision makers to ensure that the penalties remain proportionate and create meaningful deterrence. That is, just as stunt driving and racing leads to more serious consequences compared to regular speeding on a highway, in my view, the reckless exploitation of individuals using mass electronic surveillance should carry more severe penalties compared to other forms of unreasonable electronic surveillance.[1084] In this way, penalties in Canada can meet the general goal of being more effective, proportionate and dissuasive as proposed by Articles 83(9) and 84(1) of the *GDPR*,[1085] and also align more closely to what overseers in other jurisdictions are awarding in response to similar types of misconduct.[1086]

In this part, I have argued that *PIPEDA* does not provide the Privacy Commissioner of Canada with the necessary order-making powers and penalties, especially in regards to electronic surveillance. I stressed that it was not clear why the Privacy Commissioner of Canada did not have order-making powers or the ability to impose meaningful penalties, and noted that provisions in other Canadian and American jurisdictions provided these powers. I also considered the strategies of the European Union and recommended several ways to provide the Privacy Commissioner of Canada with the necessary tools for dealing with cases of noncompliance.

4.3.3 Implications for the New Workplace Privacy Regime

This analysis suggests that there are some deficiencies in *PIPEDA* when it comes to order-making powers and proportional penalties. In my view, it is necessary to address these deficiencies by removing provisions requiring the Privacy Commissioner of Canada

---

[1084] For example, in Ontario, driving a motor vehicle on a highway in a race or contest, while performing a stunt or on a bet or wager, can lead to fines between $2,000 to $10,000, the suspension of a driver's licence for a period of no more than two years (up to ten years on subsequent conviction), a seven-day vehicle impoundment, and possible imprisonment for up to six months. See *Highway Traffic Act*, RSO 1990, c H.8, ss 128(14)−(14.1), 172.
[1085] *GDPR*, *supra*, note 655 at arts 83(9), 84(1).
[1086] *Ibid* at art 83(1)−(6); Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (24 July 2019), online: *Federal Trade Commission* <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

to obtain an order from the Federal Court, and adding provisions so that the Privacy Commissioner of Canada has order-making powers. Other jurisdictions have such provisions, and I would argue that if it is to fulfill its mandate, the Privacy Commissioner of Canada must also be empowered to make orders and impose meaningful penalties in order to properly address issues of unreasonable electronic surveillance in the workplace.

4.4 Conclusion

This Chapter examined a variety of privacy provisions. I chose to focus on three themes in particular because they touched on several interesting issues relating to the electronic surveillance gap in employment. Theme 1 discussed foundational principles for understanding privacy and electronic surveillance: data collection and processing; profiling and unreasonable electronic surveillance; fair information principles; legislative purposes; privacy by design; data impact risk assessments; rights-based data protection provisions; and data fiduciaries. Theme 2 considered: definitions of consent; employees' ability to provide, withhold, and revoke consent in situations involving electronic surveillance; and strategies for facilitating an effective balance of employees' privacy interests and employers' legitimate business interests. Theme 3 dealt with order-making powers, penalties, and fines in order to strengthen the privacy regime.

I examined several Canadian privacy provisions in order to understand what currently exists in Canada and to identify any gaps that need filling with respect to electronic surveillance in the employment context. The privacy provisions I selected for Theme 1 included: *PIPEDA, Québec Charter*, and *Bill S-21 (Privacy Rights Charter).* The privacy provisions I selected for Theme 2 included: *PIPEDA, PIPEDA Breach Regulations, QC Act*, and *BC PIPA.* The privacy provisions I selected for Theme 3 included: *PIPEDA, BC PIPA,* and *QC Act.*

I specifically chose privacy provisions in the United States and the European Union in order to understand how the privacy provisions were crafted, especially for addressing situations where concepts in the theme were not covered in the Canadian privacy regime at all, which was what I found in most cases. I examined stronger provisions that

provided variety to uncover as much information as possible from the analyses and strengthen protections in Canada.

In the United States, the privacy provisions I selected for Theme 1 included: *California Consumer Privacy Act, Bill S5642 (New York Privacy Act), Bill SB 6280 (Washington Facial Recognition),* and *California Constitution.* The privacy provisions I selected for Theme 2 included: *California Consumer Privacy Act, California Labor Code,* and *California Civil Code (Customer Records).* The privacy provisions I selected for Theme 3 included: *California Consumer Privacy Act.*

In the European Union, the privacy provisions I selected for Theme 1 included: *GDPR* and *EU Convention.* The privacy provisions I selected for Theme 2 included: *GDPR.* The privacy provisions I selected for Theme 3 included: *GDPR.*

The privacy provisions fell under the three types of features of privacy provisions as mentioned in the Introduction: (1) constitutional and human rights provisions; (2) data protection provisions; and (3) employment provisions. Each of the features of privacy provisions contributed to the discussion, and was discussed within the three themes as they became relevant.

When conducting the analysis, I focused particular attention on the language and the structure of the provisions to isolate useful elements that can be used when crafting the proposed workplace privacy regime. Since the priority of this dissertation has been to identify and fill gaps in Canada's regime for the purposes of creating a new and improved workplace privacy regime, it was beneficial for me to compare similar provisions side-by-side and note subtle differences for the purposes of construction. Since the end goal was to draft a new workplace privacy regime, I examined the language of the chosen provisions to discover the various drafting strategies that could be borrowed and used to fill gaps in Canada's regime.

In this Chapter 4, the goal was not to undergo an extensive case analysis, but rather to closely scrutinize the provisions dealing with common themes to ascertain principles and values, note any beneficial construction elements, and identify any gaps in the Canadian

regime that could be filled by examining how concepts in the themes were addressed legislatively in other jurisdictions. I used this strategy so I could more effectively codify ideas when converting them into proposed provisions under the new workplace privacy regime.

This Chapter suggested that there are insufficient legislative privacy protections in Canada's legal regime compared to other jurisdictions for closing the electronic surveillance gap in employment. Moreover, principles and values were extracted from the privacy provisions, and this led to the generation of ideas that could be used to design a new workplace privacy regime to sufficiently close the electronic surveillance gap in a way that could fit into Canada's current legal system. I will discuss in Chapter 6 how I propose to fit these principles and values into Canada's legal system.

Chapter 5

5 Analysis: Examination of Workplace Privacy Cases

As mentioned in the Introduction, the purpose of this Chapter is to conduct a legal analysis of the selected workplace privacy cases of the chosen jurisdictions in order to extract useful principles and values for the purposes of designing the new workplace privacy regime and closing the electronic surveillance gap in employment.

To achieve this goal, it is important to examine workplace privacy cases of more than one jurisdiction to enable an insightful comparative analysis. Therefore, I will consider various workplace privacy cases of the selected jurisdictions, namely Canada, the United States, and the European Union.

Likewise, it is important to choose a variety of workplace privacy cases that contain several features of workplace privacy cases that provide insights into a workplace privacy situation. As mentioned in the Introduction, the key features of workplace privacy cases include: (1) employee success in the wrongful termination/privacy claim versus failure in the claim; (2) court versus labour arbitrator; (3) surveillance scenario (proactive surveillance operations versus discovery of employee misuse of technology); (4) electronic surveillance technology type; and (5) on-duty versus off-duty conduct.

Two workplace privacy cases from each jurisdiction will be discussed. The workplace privacy cases selected from Canada are: *Steel*[1087] and *Maxam Bulk Services*.[1088] The workplace privacy cases chosen from the United States are: *Graphic Packaging*[1089] and

---

[1087] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127, aff'g 2013 BCSC 527 [*Steel*].
[1088] *Maxam Bulk Services and International Union of Operating Engineers, Local 115 (Lebrun)* (2015), 2015 CarswellBC 2277 (Arbitrator: McConchie) [*Maxam Bulk Services*].
[1089] *In re Graphic Packaging International, Inc and Graphic Communications Conference International Brotherhood of Teamsters Local 77-P*, 134 LA (BNA) 369 (2014) (Wolff, Arb) [*Graphic Packaging*].

Baker Hughes.[1090] And the workplace privacy cases coming from the European Union are: *Bărbulescu*[1091] and *López Ribalda*.[1092]

The above workplace privacy cases that I have selected, based on several years of preliminary research, are significant because they contain a balanced mix of jurisdictions and a good cross-section of the features of workplace privacy cases. The selections have been made in order to avoid a skewed analysis favouring only one jurisdictional perspective (for example, exploring workplace privacy cases only from the European Union), or one kind of situation (for instance, examining workplace privacy cases decided only by courts, dealing solely with employees who are successful with their claims, looking at only one type of surveillance scenario, examining just one type of technology such as video surveillance, or investigating solely off-duty conduct). Variety can enhance the discussion and allow for the creation of a more durable workplace privacy regime.

Moreover, it is important to keep in mind that the goal of this Chapter 5 is to extract useful elements from the workplace privacy cases in order to create the new workplace privacy regime. The goal is not to provide a description of the state of the law in each jurisdiction; accordingly, I have chosen the most pertinent cases from each jurisdiction for the purposes of extracting components to generate ideas and ultimately create proposed provisions for the new workplace privacy regime. No single case can contain all of the features of workplace privacy cases; when taken together, however, these six cases provide a balanced mix of the core features of workplace privacy cases.

The workplace privacy cases I have selected also contain helpful analyses by decision makers that lead to a more effective discernment of principles and values that can be extracted for the purposes of creating a new workplace privacy regime. While some

---

[1090] *In re Baker Hughes, Inc (Claremont, OK) and United Steelworkers International Union Region VII, Local 13-391*, 128 LA (BNA) 37 (2010) (Baroni, Arb) [*Baker Hughes*].
[1091] *Bărbulescu v Romania*, Application 61496/08, Judgment of the Court (Grand Chamber), 5 September 2017, rev'g Application 61496/08, Judgment of the Court (Fourth Section), 12 January 2016 [*Bărbulescu*]
[1092] *López Ribalda and Others v Spain*, Applications 1874/13 and 8567/13, Judgment of the Court (Grand Chamber), 17 October 2019, rev'g Applications 1874/13 and 8567/13, Judgment of the Court (Third Section), 9 January 2018 [*López Ribalda*].

chosen cases are more recent than others and come from different locations within the jurisdictions, there are notably interesting aspects about each selected case that will generate new insights and enable a rich and deeper analysis and produce ingredients that I can use to make the new workplace privacy regime. These aspects are considered when delving deeper and contrasting the cases for the purposes of isolating additional relevant insights for the purpose of crafting the new workplace privacy regime. Further, there are several relevant principles stemming from employment and arbitral jurisprudence that will be discussed as they become relevant; I will refer to these principles as "employment principles".[1093] When conducting the analysis, it is also useful to understand the social reality concerning electronic surveillance and privacy that operates in the background of these cases.[1094]

There are several reasons why I have selected these six cases to examine in this dissertation. In their own way, the cases provide insights that are appropriate for studying issues related to workplace privacy in light of electronic surveillance, and making considerable contributions to the new workplace privacy regime.

The first two cases from Canada involve representative cases of the discovery of employee misuse of technology, an increasingly common phenomenon that raises a host of interesting and important issues. That said, there are some critical differences between these cases that help shed light on why one employee is successful in getting reinstated, and the other employee is unsuccessful in a wrongful termination claim where the dismissal is upheld. One case deals with a labour arbitrator and off-duty misconduct

---

[1093] To be sure, this dissertation does not aim to review all employment principles, and will only discuss the ones that become relevant to the discussion. Also important to note is that employees in workplace privacy cases are referred to as employees, grievors, or grievants, depending on the jurisdiction and unionization status. I will be referring to the name of the employees in the case, and referring to them as "employees" of the organization where applicable throughout my discussion. And when discussing collective agreements, policies, procedures, and other company rules, I collectively refer to them as "workplace documents".

[1094] Mark Van Hoecke, "Methodology of Comparative Legal Research", Law & Method (December 2015) 1 at 6−7, online: *Law and Method* <http://www.lawandmethod> DOI: <10.5553/REM/.000010>; Darren O'Donovan, "Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls" in Laura Cahillane & Jennifer Schweppe, eds, *Legal Research Methods: Principles and Practicalities* (Dublin: Clarus Press Ltd, 2016) 107 at 108, 116; Fiona Cownie & Anthony Bradney, "Socio-Legal Studies" in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 40 at 42−46, online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315386669>.

involving ubiquitous surveillance of social media, and the other deals with a court and on-duty misconduct involving the monitoring of corporate systems.

More precisely, *Steel* is a case about a senior-level employee who is terminated after improperly accessing a file on the corporate server. The case involves the discovery of misuse of technology while the employee is on-duty. *Steel* highlights core issues involving trust in the employment relationship. As well, the case focusses on the importance of balancing the legitimate interests of employers with the privacy interests of employees, and proportionality between the misconduct and the sanction imposed. *Steel* makes considerable contributions to the new workplace privacy regime in that it proposes provisions that require balanced company policies and procedures in ways that build trust in the employment relationship and ensure employees' interests are protected in workplace monitoring situations, while also protecting employers' legitimate interests to prevent the misuse of technology and consequent potential damage to the employer's reputation, clients, employees, confidential information, or property. Also, there is a focus on creating provisions that require the creation of policies and procedures that focus on the concerns of both employers and employees.

Maxam Bulk Services involves a labour arbitration. Due to a misunderstanding, the employee makes inappropriate comments on various Facebook walls using profanities. He is dismissed, but is ultimately reinstated by the arbitrator. The case deals with the discovery of misuse of technology that takes place while the employee is off-duty. This case raises a number of key issues regarding the importance of social media policies, and also draws attention to the dignity/human rights approach to privacy when examining an employee's misconduct. *Maxam Bulk Services* makes significant contributions to the new workplace privacy regime, especially when it comes to the contents of social media policies to address concerns about the use of ubiquitous surveillance that can harm an employer, an employer's clients, or the employees themselves. The proposed provisions specifically address the need to explain the disciplinary consequences of noncompliance with the policies and procedures.

The second set of cases from the United States both involve off-duty conduct, which is becoming a challenging issue given the increased sophistication of technology and prevalence of digital devices owned and used by individuals that can capture the actions of employees outside the workplace. However, although both are decided by a labour arbitrator, some of the differences in these cases explain why the arbitrator reinstates one employee, and upholds the dismissal of the other. That is, the reinstated employee is subjected to an abuse of surveillance power through proactive surveillance operations using photography and video surveillance. The extent of abuse of surveillance power in this more extreme case shows how far things can go when there are no protections in place. On the other hand, the employee who is unsuccessful in getting reinstated is discovered to have misused technology to create inappropriate online posts that are ultimately connected to the workplace policies. While this case more typically arises in the workplace, it stresses the importance of preventing inappropriate misconduct with effective company policies and procedures, and provisions in the collective agreement.

More specifically, in *Graphic Packaging*, a senior employee is wrongly suspected of being dishonest about his functional limitations following a work injury, and the employer begins electronic surveillance of him. He is reinstated, but he suffers as a result of the mistreatment. The case involves proactive surveillance operations conducted by a private investigator, which takes place while the employee is off-duty. The case touches on several employment principles, including the need for employers to respect disciplinary procedures, and have key provisions in collective bargaining agreements as well as company policies and procedures. *Graphic Packaging* makes essential contributions to the new workplace privacy regime concerning off-duty covert surveillance, the importance of knowing when to commence surveillance based on suspicion, and interpreting and responding to surveillance information. In particular, it proposes several important provisions requiring employers to respect the human dignity of employees by giving them the benefit of the doubt and attempting to understand their version of the story before hastily commencing electronic surveillance, interpreting electronic surveillance reports, and imposing discipline.

Baker Hughes involves an employee who, while off work, posts a racist blog on his MySpace account that is specifically and unquestionably aimed at one of his managers. The case involves the discovery of misuse of technology that takes place while the employee is off-duty. It deals with a labour arbitration. However, unlike what takes place in *Maxam Bulk Services*, the employee is unsuccessful in getting reinstated following a considerably different analysis that focusses on the nexus doctrine and connecting the off-duty misconduct with critical company policies and procedures, as well as the collective agreement. The case is essential for highlighting employers' responsibilities to protect employees from online harassment by their coworkers, and confirms that this is a core legitimate interest of the employer. *Baker Hughes* makes notable contributions to the new workplace privacy regime, unique to those contributed by *Maxam Bulk Services,* by focussing on the protection of the employer's own employees from each other rather than on protecting the employer's corporate reputation. *Baker Hughes* contributes to the new workplace privacy regime by proposing provisions aimed at preventing the online discrimination and harassment of coworkers with specific social media policies and procedures that set out employers' expectations regarding acceptable online use. It also enables the creation of provisions stressing that, while employees may have and use social media accounts while they are off-duty, they can never disparage coworkers and then use as an excuse that they were away from work or using their own digital devices.

The third set of cases from the European Union deals with very recent and leading court cases regarding on-duty misconduct. Yet, they contribute to our understanding of privacy in different and noteworthy ways. For instance, one deals with the discovery of misuse of instant messaging communications technology at work, and the other deals with proactive surveillance operations involving overt, covert, and also continuous video surveillance. In particular, the employee caught using instant messaging for personal reasons is ultimately successful with his privacy claim; on the other hand, the employees who are continuously monitored with overt and covert CCTV cameras are unsuccessful with their claims.

More explicitly, *Bărbulescu* concerns an engineer who works with a private company. The employee is asked to open a Yahoo! Messenger account to deal with customer concerns and after he does so, he learns that his communications have been monitored by

his employer without his knowledge. He is terminated for disobeying a company rule prohibiting the use of company equipment and communications software for personal purposes, but eventually succeeds in his privacy claim. *Bărbulescu* involves the discovery of misuse of technology and employer surveillance that takes place while the employee is on-duty; unlike a case such as *Steel* for instance, he is successful with his claim and the analysis places more emphasis on notification of the nature and extent of the electronic surveillance of electronic communications. The case highlights the importance of balancing the privacy interests of employees with the legitimate business interests of employers for the smooth operation of the business. There are core principles that emerge, such as the need to be informed of the nature, extent, and consequences of employee monitoring; I refer to these principles as the "Bărbulescu Principles" that are characteristic of the European Union's unique and novel approach. The case deals with the treatment of sensitive information, which is an important factor that requires extra attention in relation to the electronic surveillance of employees. *Bărbulescu* makes material contributions to the new workplace privacy regime and incorporates the Bărbulescu Principles to help construct essential provisions regarding the electronic surveillance of communications in the workplace.

López Ribalda is a very recent decision, involving five employees who are cashiers in a supermarket. The employer is concerned because thousands of euros of product have gone missing over five consecutive months. In response, the employer decides to conduct both overt and covert video surveillance in the workplace to catch the thieves and impose discipline. The case involves the continuous monitoring of the employees while they are on-duty. Ultimately, the employees are caught and are terminated, and unlike *Bărbulescu*, they are ultimately unsuccessful in their privacy claims in court. The case relies on and applies the Bărbulescu Principles in the consideration of electronic surveillance of employees regarding video surveillance. It also touches on important concepts related to continuous and covert video surveillance, along with the meaning of suspicion. *López Ribalda* makes important contributions to the new workplace privacy regime since there is a focus on creating provisions that incorporate the Bărbulescu Principles for the regulation of overt, covert, and continuous video surveillance of employees by employers.

As can be seen in the chart below, the examination of workplace privacy cases provides a balanced mix of jurisdictions and the features of workplace privacy cases.

Table 5: Jurisdictions and Features of Workplace Privacy Cases in Chapter 5

Jurisdiction: Canada (red) United States (blue) European Union (orange)	**Features:** **1-Employee success in the wrongful termination /privacy claim vs failure in the claim**	**2-Court vs labour arbitrator**	**3-Surveillance scenario (proactive surveillance operations vs discovery of misuse of technology)**	**4-Electronic surveillance technology type**	**5-On-duty vs off-duty**
1-*Steel* (red)	Unsuccessful (dismissed)	Court	Discovery of misuse of technology	Monitoring of corporate systems	On-duty
2-*Maxam Bulk Services* (red)	Successful (reinstated)	Arbitration	Discovery of misuse of technology	Social media	Off-duty
3-*Graphic Services* (blue)	Successful (reinstated)	Arbitration	Proactive surveillance operations	Photography and video camera	Off-duty
4-*Baker Hughes* (blue)	Unsuccessful (dismissed)	Arbitration	Discovery of misuse of technology	Social media	Off-duty
5-*Bărbulescu* (orange)	Successful (damages won)	Court	Discovery of misuse of technology	Yahoo! Instant Messaging	On-duty
6-*López Ribalda* (orange)	Unsuccessful (no damages)	Court	Proactive surveillance operations	Video surveillance (CCTV: overt, covert, continuous)	On-duty

I have discovered from preliminary research that both social media and video surveillance are more typical types of electronic surveillance technology that are used in the employment context; to that end, two of each technology types have been included in the study in order to be more representative. That said, the two selected cases differ in outcomes and analyses to better understand the principles and values emerging from those types of cases.

As with the previous Chapter 4, I attempt to respect the cultural contexts of the jurisdictions examined and find more effective ways of borrowing ideas and fitting them into the Canadian jurisdiction following a careful analysis of similarities and differences that emerge from the workplace privacy cases, for the purpose of finding practical solutions to similar problems in areas with different legal systems.[1095]

In like manner, this dissertation asks how the principles and values that emerge from selected workplace privacy cases can be used to close the electronic surveillance gap in employment using a design that fits into Canada's legal system. By "principle", I mean the ordinary meaning of the word, namely, a fundamental truth or proposition that serves as the foundation for a system of belief, behaviour, or chain of reasoning; it is the fundamental source of something.[1096] By "value", I mean the ordinary meaning of the word, namely, the regard that something is held to deserve, and the importance, worth, or usefulness of something; it includes the standards of behaviour that are judged to be important in life.[1097]

This Chapter will argue that principles and values can be extracted from all the examined workplace privacy cases, and can be used to design a new workplace privacy regime that sufficiently closes the electronic surveillance gap in a way that fits into Canada's legal system.

[1095] Geoffrey Samuel, "Comparative Law and its Methodology" in Watkins & Burton, supra note 1094, 121 at 124–134; Van Hoecke, *supra* note 1094 at 3−6, 11, 28, 30; Mathias M Siems, "The Curious Case of Overfitting Legal Transplants" in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 133 at 136−138.
[1096] Angus Stenson, ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010) *sub verbo* "principle".
[1097] *Ibid* at *sub verbo* "value".

I examine each workplace privacy case with an eye to achieving three goals. First, I thoroughly describe the workplace privacy case. Second, I analyze the case and note the principles and values that emerge from the analysis. And third, I set out my ideas for incorporating the detected principles and values into the proposed workplace privacy regime to close the electronic surveillance gap. These ideas stem from my discussion of the implications for the new workplace privacy regime. At this stage, the ideas are not yet crafted into detailed provisions. Chapter 6 will discuss how I propose to fit these ideas into Canada's legal system.

5.1 *Steel*

The first Canadian workplace privacy case that is discussed in this dissertation is *Steel*. I first describe the facts, history, and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.1.1 The Facts, History, and Decision

Susan Steel (Steel) worked with Coast Capital Savings Credit Union (Coast) as a Helpdesk Analyst in Coast's IT Department.[1098] As a Helpdesk Analyst, Steel provided internal technical assistance to other employees when they experienced network issues.[1099] Steel worked unsupervised and could access any file at Coast.[1100]

In her role, Steel was required to: follow company policies including the Code of Conduct, Conflict of Interest Policy, and Policy of Dishonest Conduct; be a positive role model and lead by example; help maintain security of the physical premises, property, and information in accordance with the internal control procedures; and respect the privacy and confidentiality of all information of customers and staff.[1101]

[1098] *Steel v Coast Capital Savings Credit Union*, 2013 BCSC 527 at para 3 [*Steel Trial*].
[1099] *Ibid.*
[1100] *Ibid.*
[1101] *Ibid.*

Coast had a policy where all employees on the internal system were assigned a personal folder that was kept on the network for the sole use of each employee.[1102] Confidential company information was put into these folders, which could only be read or edited by the individual assigned to the file.[1103] The exception to this rule was that Steel could access other employees' personal folders where she was required to assist employees with their technical problems.[1104]

There were strict rules regarding the procedure for a Helpdesk Analyst to access a file; one important feature was that Helpdesk Analysts had to obtain permission from the owner of the personal file or obtain authorization from the VP of corporate security.[1105] Steel was aware of this rule and signed that she read and understood the company Acceptable Use Policy, Code of Conduct Policy, and Information Confidentiality Policy.[1106]

Leslie Kerr (Kerr), a manager, kept a spreadsheet in her folder on priorities for the limited employee parking spaces for the IT group, which also contained confidential information such as employee pay grades and seniority dates; Steel was aware of this file and its location.[1107] In short, following a meeting regarding parking spaces, Steel went into Kerr's folder without authorization, and opened the list.[1108] Kerr complained to Steel's supervisor, Brian Vidal, when she was unable to access the file because there was a message on the screen saying that the document was already in use by Steel, and she never gave Steel permission to access the document.[1109]

Steel was immediately terminated for cause for accessing a confidential file in a private folder without permission.[1110] Steel sought damages for wrongful dismissal, and Coast

---

[1102] *Ibid* at paras 4–5.
[1103] *Ibid* at para 5.
[1104] *Ibid* at para 6.
[1105] *Ibid.*
[1106] *Ibid* at para 7.
[1107] *Ibid* at paras 8, 18.
[1108] *Ibid* at paras 19−20.
[1109] *Ibid.*
[1110] *Ibid* at para 14.

sought to have the action dismissed.[1111] Ultimately, the trial judge, Ross J., decided that Coast had just cause to terminate Steel's employment.[1112]

Steel appealed the trial decision to the Court of Appeal.[1113] Goepel J.A., writing for the majority, dismissed the appeal.[1114] The court agreed with the trial judge that *McKinley v BC Tel*[1115] applied, and stressed that a single act of misconduct could justify a dismissal if the misconduct was of a sufficient character to cause the irreparable breakdown of the employment relationship.[1116] The court confirmed that the sole issue for the trial judge was to consider whether the conduct caused a breakdown in the employment relationship, and the trial judge did not err in the analysis.[1117] More specifically, the court had to ask whether the employment relationship could no longer viably subsist, and the inherent value of the job to the employee did not need to be expressly considered in determining whether there was just cause to dismiss.[1118] Furthermore, the court stated that the trial judge was aware of the circumstances, and was open to find that there was a fundamental breakdown in the employment relationship.[1119] The appeal was dismissed.[1120]

Steel sought leave to appeal to the Supreme Court of Canada,[1121] and leave to appeal was dismissed.[1122]

5.1.2 Analysis of *Steel*

Steel involved the following features of workplace privacy cases: Steel's termination was upheld; the matter took place in a court; the surveillance scenario involved the discovery

---

[1111] *Ibid* at para 1.
[1112] *Ibid* at para 2.
[1113] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127 [*Steel Appeal*].
[1114] *Ibid* at para 18.
[1115] *McKinley v BC Tel*, 2001 SCC 38 at paras 48, 53–57 [*McKinley v BC Tel*].
[1116] *Steel Appeal*, *supra* note 1113 at para 27.
[1117] *Ibid* at paras 30, 33.
[1118] *Ibid* at paras 28−29.
[1119] *Ibid* at para 34.
[1120] *Ibid* at para 36.
[1121] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127, leave to appeal to SCC requested, 2015 CarswellBC 1979 (SCC).
[1122] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127, leave to appeal to SCC refused, 2015 CarswellBC 2649 (SCC), [2015] SCCA No 217 (SCC).

of employee misuse of technology; the technology involved the employer's corporate monitoring of systems; and the misconduct took place while Steel was on-duty.

My goal in this section is to extract principles and values from *Steel*. First, I will argue the importance of trust in both employment and data protection. Second, I will point to the critical role of balance in terms of the misconduct and the sanction imposed. And third, I will discuss the struggles faced and competing approaches used when attempting to balance the interests of the parties.

Because trust played a significant role during the analysis, it is important to examine this feature from the outset. The trial judge pointed out the critical nature of trust in this case because Coast operated in the financial industry, which is associated with higher standards when it comes to the protection of confidential information.[1123] Steel also worked with a great deal of autonomy, thus the trial judge stressed that the fundamental nature of trust was of paramount importance in this employment relationship.[1124]

The trial judge found that Steel violated the trust by opening the confidential document, and by violating the company procedures regarding remote access of the document when accessing the file without permission.[1125] Although this was not mentioned in the decision, one may question whether Steel's multiple explanations for why she needed to access the document in the first place contributed to this finding of broken trust.[1126] Steel appeared to be sneaking into a folder to snoop, since she did not have a parking spot and was one of the employees on the waiting list; she opened the confidential document right after the meeting touching on parking priorities.[1127] Both courts upheld Coast's decision to terminate Steel, a long-term employee working with Coast for 21 years.[1128]

When trust disappears in the employment relationship, the parties experience feelings of violation and betrayal that lead to a complete breakdown in the relationship, where the

---

[1123] *Steel Trial, supra* note 1098 at paras 24–25.
[1124] *Ibid.*
[1125] *Ibid* at para 28.
[1126] *Ibid* at paras 10–11.
[1127] *Ibid* at paras 8, 18–19.
[1128] *Ibid* at para 29; *Steel Appeal supra* note 1113 at para 36.

human reaction is immediate and can lead to feelings of disgust.[1129] Trust is a core aspect of the employment relationship, and when trust is broken, it is common for terminations to be upheld, even for what could be viewed as minor breaches.[1130] Trust is essential in the employment relationship to achieve harmonious workplace relations, especially given the imbalance of power that weighs in favour of employers.[1131] This inherent unequal bargaining power involves virtually all facets of the employment relationship.[1132]

It has been noted in unionized cases that a breach of trust conveys the gravity of certain misconduct whose main defining characteristic is dishonesty, such as theft, falsification of time-keeping, attendance or production records, and benefits fraud. [1133] Other examples include: failure to follow prescribed procedures for handling money or other assets; misuse of one's position to derive some illicit gain for oneself, family, or friends; gross dereliction of duty as it affects the interests of the employer's clients, customers, patients or others; engaging in an inappropriate personal or business relationships that could compromise the employer's interests; misrepresenting the reasons for requesting a leave of absence; malingering while on sick leave or long-term disability leave or providing inaccurate medical information; and failure to advise the employer of the revocation of a licence or professional certification required to carry out a job.[1134]

In nonunionized workplaces such as in this case, when courts determine whether there has been an irreparable breakdown of the relationship, they consider factors such as the context and the seriousness of the dishonesty; to decide whether there has been an

---

[1129] Donna Hicks, *Leading with Dignity: How to Create a Culture that Brings out the Best in People* (Michigan: Yale University Press, 2018) at 95−96.
[1130] Melanie R Bueckert, *The Law of Employee Monitoring in Canada* (Markham: LexisNexis Canada Inc, 2009) at 11–12.
[1131] *Machtinger v HOJ Industries Ltd*, [1992] 1 SCR 986 at para 31, 1992 CarswellOnt 892 (SCC) [*Machtinger*]. See also David J Doorey, *The LAW of Work: Common Law and the Regulation of Work* (Toronto: Emond Montgomery Publications Limited, 2016) at 5−6, 67−75, 111−120 [David Doorey, "Common Law and Regulation"]; David J Doorey, *The LAW of Work: Industrial Relations and Collective Bargaining* (Toronto: Emond Montgomery Publications Limited, 2017) at 67, 94−97, 239−241 [David Doorey, "Industrial Relations and Collective Bargaining"].
[1132] *Wallace v United Grain Growers Ltd*, [1997] 3 SCR 701 at paras 92−93, 1997 CarswellMan 455 (SCC) [*Wallace*].
[1133] Morton Mitchnick & Brian Etherington, *Labour Arbitration in Canada*, 3rd ed (Toronto: Lancaster House, 2018) at 333.
[1134] *Ibid* at 333–334.

irreparable undermining of trust that is required in the employment relationship, courts are likely to set a higher standard for employees when they work in roles involving a great deal of autonomy, positions of authority, or positions requiring special trust.[1135]

When misusing company technology, employees typically access the information of coworkers, clients, or the employer; regardless of the type of misconduct, the motivations are primarily to engage in various illegal or unethical activities for personal gain, or to damage the employer's property, information, or reputation.[1136] With respect to data breaches alone, about 33 percent of reported breaches are caused by an insider who is typically an authorized individual with valid credentials within the organization.[1137] Furthermore, in organizations that experience economic crime and fraud, more than half of the perpetrators are internal actors.[1138] In other words, not every invasion comes from a malicious external attacker, and it is necessary to focus on misuse of technology by authorized individuals.[1139]

Cyber security incidents have serious financial consequences; Statistics Canada has found that Canadian businesses reported spending approximately $14 billion to prevent, detect

---

[1135] David Doorey, "Common Law and Regulation", *supra* note 1131 at 175.
[1136] Paul Healy & George Serafeim, "How to Scandal-Proof Your Company: A Rigorous Compliance System is Not Enough" *Harvard Business Review* (July–August 2019), 42 at 42–50.
[1137] Buckley Smith, "Laying Blame on Employee in Desjardins Data Breach is Ignoring the Big Picture, Security Experts Say" (21 June 2019), online: *ITWorldCanada* <https://www.itworldcanada.com/article/laying-blame-on-employee-in-desjardins-data-breach-is-ignoring-the-big-picture-security-experts-says/419299>.
[1138] Healy & Serafeim, *supra* note 1136 at 44. This finding comes from a 2009 PwC survey of approximately 7,000 organizations that experienced economic crime and fraud in the previous year.
[1139] B Smith, *supra* note 1137.

and recover from cyber security incidents in 2017.[1140] 21 percent of businesses reported they were impacted by a cyber security incident that affected their operations.[1141]

It appears that banking institutions need to better protect their data compared to businesses operating in other industries. For instance, banking institutions were more likely to be impacted by cyber security incidents and reported some of the highest levels of incidents at 47 percent, which prevented employees from working, created downtime, and added repair or recovery costs; this may explain why 81 percent of banking institutions were required to implement cyber security measures by their suppliers, customers, partners or regulators in 2017 compared to 29 percent of businesses overall.[1142] While 13 percent of businesses had a written policy in place to manage or report cyber security incidents overall, 66 percent of banking institutions had such a written policy.[1143] And whether the motives were to steal money, demand a ransom payment, access unauthorized areas, or steal personal or financial information, 65 percent of businesses reported that they believed an external actor was involved, and thus it can be deduced that 35 percent believed an internal actor was involved.[1144]

When it comes to dealing with internal actors, most of whom are employees, recent research suggests that an effective strategy is to go beyond using strong compliance systems, and address root causes of the problem that involve leadership and corporate culture; employers can combat illicit employee behaviour, such as what took place in the

---

[1140] Statistics Canada, "Impact of Cybercrime on Canadian Businesses, 2017" (15 October 2018) at 1, online (pdf): *Statistics Canada: The Daily* <https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm>. A survey was launched to further understand the impact of cybercrime on Canadian businesses including aspects such as investment in cyber security measures, cyber security training, the volume of cyber security incidents, and the costs associated with responding to these incidents. The target population was derived from Statistics Canada's Business Register, which is an information database on the Canadian business population and serves as a frame for all Statistics Canada business surveys. It is a structured list of businesses engaged in the production of goods and services in Canada in almost all industrial sectors. The survey data are collected using an electronic questionnaire, and the number of enterprises within the target population was 197,019 enterprises.
[1141] Statistics Canada, *supra* note 1140 at 1.
[1142] *Ibid* at 1−2.
[1143] *Ibid.*
[1144] *Ibid* at 1.

recent Desjardins data breach,[1145] by setting social norms within the organization and managing the risk of misconduct.[1146] Further, it is important to send a message that misuse of personal information is unacceptable and the policies and procedures prohibiting this misconduct will be consistently enforced.[1147] Organizations need to actively recruit and promote managers who value integrity, and create policies and procedures that reduce the opportunity for committing unethical acts.[1148]

On the issue of data breaches alone, the Office of the Privacy Commissioner of Canada has recently reported that, between November 1, 2018 and October 31, 2019, the Privacy Commissioner received 680 breach reports, and the number of Canadians who have been affected by a data breach was over 28 million;[1149] this number included two major data breaches that occurred during this time period, namely the Desjardins and Capital One breaches.[1150] In fact, 58 percent or 397 breach reports involved unauthorized access, some of which was caused by employee snooping and social engineering hacks such as phishing and impersonation.[1151]

[1145] Jonathan Montpetit, "Personal Data of 2.7 Million People Leaked from Desjardins" (20 June 2019), online: *CBC News Montreal* <https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297>.

[1146] Healy & Serafeim, *supra* note 1136 at 44–45. For 10 years, the authors explored how companies can create an environment that discourages illicit activities including white-collar crime, using data from individual companies and from surveys by PwC, Transparency International, the World Bank, executive recruiting firms, and other organizations. They looked at data on thousands of organizations and individuals, and interviewed more than 50 senior and middle managers at 10 organizations that have experienced scandals. The main finding was that while compliance systems were important, leadership played a critical role in shaping organizations attitude toward preventing crime and responses when wrongdoings are detected.

[1147] Healy & Serafeim, *supra* note 1136 at 45.

[1148] *Ibid*.

[1149] Office of the Privacy Commissioner of Canada, "A Full Year of Mandatory Data Breach Reporting: What We've Learned and What Businesses Need to Know" (31 October 2019), online (blog): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/blog/20191031/> [Privacy Commissioner, "Breach Reporting"].

[1150] Office of the Privacy Commissioner of Canada, "Quebec, Federal Privacy Commissioners Investigate Desjardins Breach" (8 July 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190708/>; Office of the Privacy Commissioner of Canada, "OPC Launches Investigation into Capital One Breach" (31 July 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190731_02/>.

[1151] Privacy Commissioner, "Breach Reporting", *supra* note 1149. It is important to recognize that some instances were merely due to employee error; 147 out of 680 breaches were due to accidental disclosure.

Organizations are recommended to balance entrepreneurship and responsibility by creating a code of conduct and asking employees to follow it.[1152] It is also important to have internal and external whistleblower systems to ensure behaviour remains consistent with the company vision.[1153] An essential indicator of an ethical culture is when an organization has a zero-tolerance policy for wrongdoing; when members of upper management break the rules, it is necessary for these managers to be punished in the same manner as other employees who break the rules.[1154] Organizations can help employees develop moral humility, which is the recognition that we all have the capacity to transgress if we are not careful.[1155] When it comes to ethics in the workplace, it is recommended that there be a development of a three-stage approach: (1) prepare in advance for moral challenges to overcome the bias of overestimating the virtuousness of our future selves using strategies such as goal setting and if-then planning; (2) make good decisions in the moment by stepping back, searching for moral issues, and exploring ethical implications; and (3) reflect on and learn from moral successes and failures for the purposes of future growth.[1156]

It seems evident that organizations have a legitimate business interest in protecting client and employee information, as well as employer information, property, and reputation; one way to accomplish this goal is to approach management with the aim of creating an ethical workforce. It may be useful to support organizations in building ethical workplaces and view this as a strong legitimate business interest.

In this case, Coast was upholding cherished company values and enforcing its own clear policies and procedures, of which Steel was aware.[1157] Coast did not lessen the penalty merely because Steel was in a more senior position, or because the file she accessed had

---

[1152] Harvard Business Review, "We Were Coming Up Against Everything from Organized Crime to Angry Employees" *Harvard Business Review* (July–August 2019), 54 at 55–56.
[1153] *Ibid.*
[1154] Mary Jo White, "What I've Learned about White-Collar Crime" *Harvard Business Review* (July–August 2019), 58 at 59.
[1155] Maryam Kouchaki & Isaac H Smith, "Building an Ethical Career: A Three-Stage Approach to Navigating Moral Challenges at Work" *Harvard Business Review* (January−February 2020), 135 at 135.
[1156] *Ibid* at 135−139.
[1157] *Steel Trial, supra* note 1098 at para 14.

to do with employee parking spaces; instead, Coast took the approach that it was important to treat all employees who engaged in dishonesty equally in order to send a message that this type of misconduct would not be tolerated.[1158] Coast bolstered the integrity of its workforce, and the courts supported it.[1159]

To recap, I have just explained the importance of trust in employment and data protection. The second thing that I will do is delve into the concept of balance regarding the misconduct and the sanction imposed.

To that end, the trial judge first referred to *McKinley v BC Tel,*[1160] and highlighted that, considering the need to use a contextual analysis and the principle of proportionality, there had to be a balance struck between the severity of the misconduct and the sanction imposed.[1161] While the trial judge emphasized that terminations constituted the most severe punishment in employment and were reserved for only the most serious kind of misconduct, there were instances where a termination was appropriate, and the question was ultimately whether there was an irreparable breakdown of the employment relationship.[1162] In this case, Steel was found to have engaged in dishonesty that led to a breakdown in the employment relationship, which was evident when examining Coast's language in the termination letter, stating that Steel's actions "flew in the face of the trust"[1163] that was required in the position involving access to confidential and private information.[1164] Coast even used the phrases such as, "serious loss of confidence"[1165] and "irreparably damaged the employment relationship".[1166]

The Court of Appeal confirmed the trial judge's decision, and stated that the only issue to address was whether the conduct caused a breakdown of the employment relationship; the court was not willing to perform an extensive analysis of additional surrounding

---

[1158] *Ibid.*
[1159] *Ibid* at para 2; *Steel Appeal, supra* note 1113 at para 18.
[1160] *McKinley v BC Tel, supra* note 1115 at paras 48, 53−57.
[1161] *Steel Trial, supra* note 1098 at para 22.
[1162] *Ibid*.
[1163] *Ibid* at para 14
[1164] *Ibid.*
[1165] *Ibid.*
[1166] *Ibid.*

factors that were raised by the dissenting judge, Donald J.A.[1167] The Court of Appeal held that the seriousness of the misconduct violated the trust in the employment relationship and caused an irreparable breakdown of the employment relationship.[1168] The Court of Appeal made it clear that the trial judge considered all the relevant factors when performing the balancing process; in this case however, the positive aspects of Steel's employment, such as length of service, were outweighed by the severity of the misconduct, namely the breach of trust in this case.[1169] In fact, the Court of Appeal highlighted several of the factors that justified the trial judge's decision, including the seriousness of the misconduct, policies on privacy-related matters, and the trust that was violated, and confirmed that the trial judge was open to find a fundamental breakdown in the employment relationship.[1170]

I have therefore shown the noteworthy aspects of balance in terms of the misconduct and the sanction imposed. The third thing that I will do is illustrate the consequential struggles that arise and the competing approaches used when attempting to balance the interests of the parties.

To this end, it is worth noting that the dissent in the case was substantial.[1171] More explicitly, Donald J.A. disagreed with the analyses of both the trial judge and the majority of the Court of Appeal, mainly because the dissenting analysis aimed at examining more than just whether the severity of the misconduct and the sanction imposed were proportionate.[1172] In the discussion concerning proportionality, the dissent focused on additional factors that had to be considered given the wider appreciation of the employment relationship; these factors included the inherent value of the job to the employee, length and quality of service, and the unequal bargaining power that put employees in a vulnerable position.[1173] The dissenting judge even referred to the Dickon

---

[1167] *Steel Appeal*, *supra* note 1113 at paras 28−30.
[1168] *Ibid* at para 27.
[1169] *Ibid* at paras 28−29, 34.
[1170] *Ibid*.
[1171] *Ibid* at paras 1−17.
[1172] *Ibid* at para 10.
[1173] *Ibid* at paras 10–11.

dissent,[1174] and insisted that it was important to use a more humane approach during the analysis.[1175] Donald J.A. referred to the range of sanctions in the policy that could apply in instances of noncompliance, and asserted that it was not fair to allow one instance of a breach of privacy rules to end a 21-year career.[1176]

When reviewing the decision at both levels, there appears to be a struggle between the idea of an organization using strict rules to ensure the protection of confidential information stored on its server, and the contention that employment principles should be used to support saving the job of a long-term employee who made a single mistake. What can be taken from this case is that it is not an easy balance to strike—these opposing interests are valid, and there is no easy answer. Employing a balancing exercise appears to be one of the most effective strategies for dealing with the challenge of resolving strong opposing interests, but this means that a judge or a labour arbitrator uses discretion and performs the balancing, deciding which interests carry more weight. One thing that can be said is that company policies and procedures play a large role during this decision-making process.

In this part, I extracted principles and values from *Steel*. I did this by discussing trust, balance with respect to the misconduct and the sanction imposed, and the challenge of balancing the interests of the parties. It is important to stress that, since the notion of trust will act as a through-line for all cases that I will be discussing, I spent a considerable amount of time examining it in my analysis of this first case. As will be seen throughout this dissertation, when there is a violation of trust in the employment relationship, there is a strong likelihood that there will be consequent feelings of betrayal.

5.1.3 Implications for the New Workplace Privacy Regime

What the above analysis suggests is that there are a few themes that are present in workplace privacy cases that need to be addressed when creating provisions in the new

---

[1174] *Reference Re Public Service Employee Relations Act (Alta)*, [1987] 1 SCR 313 at para 95, 1987 CarswellAlta 705 (SCC) [*Alberta Reference*].
[1175] *Steel Appeal*, *supra* note 1113 at para 11.
[1176] *Ibid* at paras 12, 15.

workplace privacy regime. For example, trust and balance are core features of the employment relationship and also in data protection. Thus, there needs to be the creation of provisions that require a balancing of opposing interests of the parties in a way that aims to build trust in the employment relationship; for example, this can be accomplished by requiring the creation of fair policies and procedures where employees are protected from unreasonable electronic surveillance, and employers' legitimate interests are also protected in order to prevent the misuse of technology, including data breaches and illicit behaviour, which could lead to damage to the employer's reputation, clients, employees, or property. Given the inconsistencies associated with data protection and employment principles, it is also necessary to ensure that there is a fair balancing to resolve strong opposing interests in an employment relationship. Thus, it is necessary to create provisions that require the creation of policies and procedures that focus on the concerns of both employers and employees.

5.2 *Maxam Bulk Services*

The second Canadian workplace privacy case that is discussed in this dissertation is *Maxam Bulk Services.* I first describe the facts and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.2.1 The Facts and Decision

Sheldon Lebrun (Lebrun) had been employed with Maxam Bulk Services (Maxam), a manufacturer and distributor of explosives, for four and one half years.[1177] Maxam had one main customer, Teck Coal Limited (Teck), which made up 90 percent of its business in Canada; without Teck, Maxam would not be operating in this location. One of the tasks Lebrun performed in his role as spare lead hand was to record any safety concerns at the site on a daily basis.[1178] Lebrun noted over many months that there was a deficiency, namely there was a malfunction of one of the two electric gates that protected

[1177] *Maxam Bulk Services, supra* note 1088 at paras 4, 8.
[1178] *Ibid* at para 11.

the site silo from wandering animals.[1179] One part of a gate had been severed accidentally, and since the deficiency had not been fixed, the silo was exposed to encroachment by animals.[1180] Though Lebrun noted this deficiency repetitively, no improvements were made, and eventually some sheep got into the silo enclosure, consumed some chemicals, and died.[1181]

Lebrun learned about the deaths the next day when his supervisor called.[1182] For some unknown reason, Lebrun got the impression from his supervisor during this call that the main client, Teck, was blaming Maxam for the sheep deaths.[1183] In response, Lebrun became frustrated because he thought that Maxam was being accused, and he believed that the real problem was Teck's failure to repair the gate.[1184] Over a few days, Lebrun posted inappropriate comments on several Facebook walls while he was at home and off-duty; he criticized Teck and his supervisor, used highly offensive swearwords aimed directly at Teck, and ranted about how Teck was not taking responsibility for what happened to the sheep.[1185] The VP of Maxam learned about the posts when he received a phone call from Teck's general manager, and was directed to the posts that were on Lebrun's wall; he could easily see the posts since Lebrun did not use any privacy settings.[1186] Maxam apologized to Teck and dismissed Lebrun.[1187]

At the grievance, Maxam argued that the discharge should be upheld and the grievance should be dismissed.[1188] Maxam argued that Lebrun broke the trust with Maxam, damaged the relationship between Maxam and Teck, damaged Teck's reputation, and slandered his supervisor.[1189] Maxam asserted that there was no serious expectation of privacy regarding the Facebook posts, and although Lebrun claimed that he did not know

---

[1179] *Ibid* at para 12.
[1180] *Ibid.*
[1181] *Ibid* at para 14.
[1182] *Ibid* at para 15.
[1183] *Ibid.*
[1184] *Ibid.*
[1185] *Ibid* at paras 17–24.
[1186] *Ibid* at paras 17–18.
[1187] *Ibid* at paras 27, 44–45, 47.
[1188] *Ibid* at para 79.
[1189] *Ibid* at para 80.

the comments were public, ranting without being aware of the privacy settings was reckless.[1190] Maxam also argued that Lebrun's off-duty conduct met the test in *Millhaven Fibres*[1191] for discipline for off-duty conduct.[1192] In contrast, the union argued that, though there was cause for some discipline, the termination was excessive in all of the circumstances, and reinstatement was appropriate.[1193] For Lebrun, posting on Facebook was more like having a beer with a friend and complaining about work.[1194] He had honestly not turned his mind to his Facebook privacy settings, and this was very common among Facebook users.[1195] Also, if Maxam had a social media policy, Lebrun would have better understood that his conduct was serious and that Facebook was not the place to complain about the workplace.[1196]

The arbitrator, McConchie, proceeded to examine the relevant mitigating and aggravating factors.[1197] For instance, Lebrun was a very good employee who was middle of the seniority list, and this incident was considered to be shocking.[1198] The arbitrator considered Lebrun's attitude, honesty, demonstration of remorse, and clean record and

---

[1190] *Ibid* at paras 83–86.
[1191] *Millhaven Fibres Ltd, and Oil, Chemical & Atomic Workers Int'l Union, Local 9-670* (Arbitrator: Anderson), cited in *Re Lethbridge (City) and ATU, Loc 987 (Grant)* (2000), 98 LAC (4th) 264 (Arbitrator: Tettensor) at 278–279 [*Millhaven Fibres*]. See also *Re Wasaya Airways LP and Air Line Pilots Association, International (Wyndels)* (2010), 2010 CarswellNat 6233, [2010] CLAD No 297 (Arbitrator: Marcotte). The test is: discharge for off-duty misconduct will be sustained if the employer can show that: (1) the conduct harmed the employer's reputation or product; (2) the employee's behaviour rendered the employee unable to perform duties satisfactorily; (3) the employee's behaviour leads to a refusal, reluctance, or inability of the other employees to work with the employee; (4) the employee has been guilty of a serious breach of the *Criminal Code* and renders his conduct injurious to the general reputation of the employer and its employees; or (5) the situation places difficulty in the way of the employer properly carrying out its function of efficiently managing its works and efficiently directing its working forces. The general consensus among arbitrators is that it is not necessary for an employer to show that all the criteria exist, but rather that, depending on the degree of impact of the offence, any one of the consequences may warrant discipline or discharge.
[1192] *Maxam Bulk Services, supra* note 1088 at paras 88–104.
[1193] *Ibid* at paras 123–124.
[1194] *Ibid* at para 135.
[1195] *Ibid.*
[1196] *Ibid* at para 136.
[1197] *Ibid* at paras 149–151. See also *Re United Steelworkers of America, Local 3257 and the Steel Equipment Co Ltd* (1964), 1964 CarswellOnt 498 at 2, [1964] OLAA No 5 (Arbitrators: Reville, Park & White); *William Scott & Co and Canadian Food and Allied Workers Union, Local P-162*(1976), 1976 CarswellBC 518 at paras 9−12, [1976] 2 WLAC 585 (Arbitrators: Macdonald, Alcott & Weiler).
[1198] *Maxam Bulk Services, supra* note 1088 at paras 154−155.

concluded that this was an isolated incident.[1199] The arbitrator noted that there was an element of premeditation since Lebrun chose to demonstrate his anger on Facebook.[1200] Further, the arbitrator stated that the seriousness of the offence was a major factor in this case; Lebrun engaged in a brief but offensive campaign which slurred his own company's sole customer, criticized his employer, and involved insubordinate comments about one of his supervisors.[1201] However, the arbitrator stated that it was notable that Lebrun apologized to Maxam, tried to apologize to Teck, and he would have apologized to his supervisor had he run into him.[1202] The arbitrator discussed the significance of the absence of a social media rule or policy; while it was not an excuse for Lebrun, it did remove from Maxam's "quiver of reasons for upholding the dismissal"[1203] that Lebrun knew what was expected of him and the consequences of breaching that expectation.[1204] And there were no attempts of earlier, more moderate forms of corrective discipline.[1205]

Ultimately, the arbitrator stressed that, though Lebrun's misconduct was serious, it was not so serious that it should override the opportunity for progressive discipline for the benefit of the continued employment relationship.[1206] The arbitrator briefly compared other instances of social media rants, and concluded that Lebrun's misconduct was not as serious, relatively speaking.[1207] There was a low risk of recurrence given that there was no violence or disparagement of other races and genders, and the motivation for ranting on social media was dissimilar from other cases since Lebrun thought his employer was unfairly treated.[1208] The arbitrator reinstated Lebrun.[1209]

[1199] *Ibid* at paras 156–159.
[1200] *Ibid.*
[1201] *Ibid* at paras 166, 191.
[1202] *Ibid* at paras 167, 175–176, 180.
[1203] *Ibid* at para 168
[1204] *Ibid*.
[1205] *Ibid* at para 170.
[1206] *Ibid* at para 191.
[1207] *Ibid* at paras 184–189.
[1208] *Ibid* at paras 192–196.
[1209] *Ibid* at paras 199–202.

5.2.2 Analysis of *Maxam Bulk Services*

This case involved the following features of workplace privacy cases: Lebrun was successful in being reinstated; the matter involved a labour arbitration; the surveillance scenario involved the discovery of employee misuse of technology; the electronic surveillance technology involved social media, namely Facebook; and the misconduct took place while Lebrun was off-duty.

This case is interesting when comparing it to the previous case, *Steel*, since it had the exact opposite result. Steel worked with her employer for 21 years, accessed a file regarding employee parking spaces without permission, was terminated immediately with no notice, and was unsuccessful in her wrongful dismissal claim. In contrast, in *Maxam Bulk Services,* Lebrun worked with his employer for just four and one half years, made inappropriate posts on Facebook that were filled with profanities and aimed directly at the employer's main client and his supervisor, was dismissed, and was subsequently reinstated by the arbitrator. Both employers had something at stake, including confidential information and online reputation.

One reason for the difference in results could be that one case was resolved in courts, whereas the other was resolved in a labour arbitration. In my view, this made a significant difference because labour arbitrators tend to take relatively more time to thoroughly examine the entire situation and give the employee the benefit of the doubt before making any decisions about whether a dismissal should be upheld or substituted with a lesser penalty. For instance, the trial judge in *Steel* briefly noted the relevant legal principles in four paragraphs and subsequently made a decision in a discussion that lasted four paragraphs;[1210] similarly, the majority in the Court of Appeal in *Steel* briefly decided in a discussion that lasted 10 paragraphs.[1211] Conversely, the arbitrator's discussion in *Maxam Bulk Services* lasted a considerable 62 paragraphs, where the arbitrator considered the entire context when examining each and every aggravating and mitigating

---

[1210] *Steel Trial, supra* note 1098 at paras 21–29.
[1211] *Steel Appeal, supra* note 1113 at paras 26–36.

factor.[1212] It appears that there may have been a more genuine attempt to understand the situation from Lebrun's perspective and to use a more humane approach, where there was a wider appreciation of employment principles described by Donald J.A. in the Court of Appeal dissent in *Steel*.[1213]

In addition, there was a difference in industry type (banking versus mining); as discussed in *Steel*, standards appear to be high when it comes to the protection of confidential information in the banking industry. Still, I believe that another crucial reason why these cases were so different had to do with the question of whether there was a strong company policy and set of procedures, as I will demonstrate below.

My goal in this section is to extract principles and values from *Maxam Bulk Services*. First, I will emphasize the importance of having a social media policy. Second, I will explain the use of the dignity/human rights approach to privacy. And third, I will discuss critical employment principles such as balancing mitigating and aggravating factors, progressive discipline, and the test for discipline involving off-duty conduct.

Thus, I will first mention that this case highlighted the impact of having a company social media policy. More precisely, Lebrun argued that Maxam did not have a social media policy, and had there been one, he would have better understood the ramifications of his behaviour, known that it was not acceptable to complain about work online, and been aware that there were serious consequences.[1214] The arbitrator clearly stated that, without having a rule or policy governing social media use, Maxam's support for upholding the dismissal was weakened because Lebrun did not know exactly what was expected of him or the consequences of breaching those expectations.[1215] Plainly put, it is critical for employers to have these policies and procedures setting out the company rules for Internet use, because decision makers refer to these policies and procedures when deciding whether to uphold a dismissal.[1216] In fact, I believe that Steel was unsuccessful

---

[1212] *Maxam Bulk Services, supra* note 1088 at paras 140–202.
[1213] *Steel Appeal, supra* note 1113 at para 11.
[1214] *Maxam Bulk Services, supra* note 1088 at para 136.
[1215] *Ibid* at para 168.
[1216] *Ibid.*

with her claim because Coast had crystal clear policies and procedures that it took very seriously, which Steel breached; in contrast, Lebrun did not seem to understand what the rules were because there was no policy.[1217]

In modern times, social media use and mobile devices have created an explosion of possibilities to monitor individuals.[1218] In particular, every time we post personal information online, we inadvertently participate in our own surveillance because information can be easily captured by anyone.[1219] We cannot escape ubiquitous surveillance, and it is important to be aware of the data trails that are left behind and the digital persona that we are creating as a consequence of our browsing and participating in online activity.[1220] This is because the data proxies that are built over time paint a virtual portrait of a person, typically for the purposes of establishing positive social relations and identities, avoiding any data-derived harm, and enhancing autonomy.[1221] We as a society have come to accept that we live in a surveillance society where the culture of surveillance involves our daily lives being recorded, monitored, and tracked through online interactivity and user-generated surveillance, to the point where it has been taken for granted.[1222]

However, ubiquitous surveillance creates a potential for differential treatment and the exploitation of individuals through the abuse of surveillance power, especially when there are asymmetrical power relations involved between the watchers and the watched.[1223]

[1217] *Steel Trial*, *supra* note 1098 at paras 48–49; *Steel Appeal*, *supra* note 1113 at 27; *Maxam Bulk Services*, *supra* note 1088 at para 136.
[1218] Colin J Bennett et al, *Transparent Lives: Surveillance in Canada* (Edmonton: AU Press, Athabasca University, 2014) at ix [Bennett et al, "Transparent Lives"].
[1219] *Ibid* at 170–171.
[1220] Roger Clarke & Graham Greenleaf, "Dataveillance Regulation: A Research Framework" (2017) 25:1 J L Info & Sci 104 at 105–106, 108; Gavin JD Smith, "Surveillance, Data and Embodiment: On the Work of Being Watched" (2016) 22:2 Body & Society 108 at 110–111, 119, online (pdf): *SAGE Publishing* <bod.sagepub.com> DOI: <10.1177/1357034X15623622>.
[1221] G Smith, *supra* note 1220 at 110–111, 119.
[1222] David Lyon, *The Culture of Surveillance* (Cambridge: Polity Press, 2018) at 30, 83 [David Lyon, "Culture of Surveillance"].
[1223] Mark Andrejevic, "Automating Surveillance" (2019) 17:1/2 Surveillance & Society 7 at 7–9, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> [Mark Andrejevic, "Automating Surveillance"].

One consequence is the potential for differential treatment in cases such as stalking and violence against women.[1224]

And when it comes to employment, where the watcher is the employer, the information we leave behind in the online world when we expose ourselves by leaving electronic traces can be collected, linked together, and amalgamated, can be used against us to punish us.[1225] Furthermore, when we "share" all types of information online, we expose ourselves and become virtually transparent to anyone, and leave traces for all to see and use—including employers.[1226]

This case discussed how Maxam was able to easily access Lebrun's information from the outside world on Facebook, and use it to make disciplinary decisions in employment.[1227] This is why it is so important to establish clear company social media policies and procedures in order to set some standards as to what is and is not acceptable, and explain the consequences for noncompliance.[1228]

In fact, the Office of the Privacy Commissioner of Canada stresses that there are privacy concerns when employees use social media, and employees should be aware that any of the information or communications posted on their social media can potentially be accessed by current or potential employers; recruitment agencies; co-workers; the employer's competitors; government and law enforcement agencies; and others outside the employee's trusted network.[1229] And when it comes to monitoring social media use, employees should know that, subject to existing workplace policies and rules, some organizations monitor their employees' social media, and thus, they should be aware that

---

[1224] Corinne Mason & Shoshana Magnet, "Surveillance Studies and Violence Against Women" (2012) 10:2 Surveillance & Society 105 at 106–107, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> [Mason & Magnet, "Surveillance Studies and Violence"].
[1225] Bernard E Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015) at 13–14.
[1226] *Ibid.*
[1227] *Maxam Bulk Services, supra* note 1088 at paras 44–47.
[1228] *Ibid* at para 168.
[1229] Office of the Privacy Commissioner of Canada, "Privacy and Social Media in the Workplace" (August 2019), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_41_sn/> [Privacy Commissioner, "Social Media"]..

when using social media in a workplace context, their personal information may be collected, used and disclosed by the employer (including off-duty comments and postings).[1230] The employers and employees should be aware of the potential damages to individuals and the organization through inappropriate disclosures of personal or confidential business information on social media, some of which include: defamation lawsuits; copyright, patent or trademark infringement claims; privacy or human rights complaints; workplace grievances under a collective agreement or unfair labour practice complaints; criminal charges with respect to obscene or hate materials; and damages to the employer's reputation and business interests.[1231] Therefore, the Office of the Privacy Commissioner of Canada recommends developing and communicating a clear policy on social media; employers should inform employees in plain language why they should keep some personal and corporate information confidential or undisclosed.[1232] Further, the policy should address: whether the organization permits the use of personal or employer-hosted social media in the workplace; where social media accounts are permissible, the context and purposes that they be used; whether the employer monitors social media sites; what legislation applies to the collection, use or disclosure of personal information in the workplace; what other rules (for example, contract or collective agreement) may apply to the use of social media in the workplace; the consequences of non-compliance with the policy; and any other existing policies about the proper use of electronic networks with respect to employee privacy and handling confidential information.[1233] I would like to suggest that these recommendations for creating social media policies and also policies dealing with related topics such as privacy and security issues with personal digital devices in the workplace[1234] be incorporated into the new workplace privacy regime.

[1230] *Ibid.*
[1231] *Ibid.*
[1232] *Ibid.*
[1233] *Ibid.*
[1234] Also important to note is that the Office of the Privacy Commissioner of Canada has created tips for organizations who wish to protect privacy on mobile devices and who are contemplating a Bring Your Own Device Program. See Privacy Commissioner, "BYOD Program the Right Choice?", *supra* note 842; Office of the Privacy Commissioner of Canada, "10 Workplace Tips for Protecting Personal Information on Mobile Devices" (January 2011), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-

I have just argued for the conclusion that it is important to have a social media policy. The second thing that I will do is examine the specific discussion about privacy and the arbitrator's use of the dignity/human rights approach to privacy when making the decision.

More specifically, Lebrun argued that, when he posted on Facebook, it was more like having a beer with a friend and complaining about work.[1235] Moreover, he said that he had honestly not turned his attention to his Facebook privacy settings, and he was not quite sure whether his posts were public or private.[1236] Maxam argued that, given the profanities Lebrun used, this behaviour of posting without checking privacy settings was reckless.[1237] Despite the severity of the misconduct and Lebrun's lackadaisical attitude toward checking Facebook privacy settings, the arbitrator briefly noted at the end of the analysis that Lebrun's posts were not as serious as most rants on the Internet, since the comments did not display violence or disparagement of other races and genders, and the motivation for the rants was to blow off steam after he thought Maxam was being unfairly treated.[1238]

---

work/02_05_d_46_dpd/>; Office of the Privacy Commissioner of Canada, "Contemplating a Bring Your Own Device (BYOD) program?" (August 2015), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/tips_byod/>. Employers who are contemplating a BYOD program are recommended to: (1) Get executive buy-in for BYOD privacy protection; (2) Assess privacy risks; (3) Establish a BYOD policy; (4) Pilot the program; (5) Train staff; (6) Demonstrate accountability; (7) Mitigate risks through containerization; (8) Put in place storage and retention policies; (9) Encrypt devices and communications; (10) Protect against software vulnerabilities; (11) Manage apps effectively; (12) Enable effective authentication and authorization practices; (13) Address malware protection; (14) Have a plan for when things go wrong. For a BYOD Program, employers are recommended to, among other things: conduct a privacy impact and threat risk assessment; create a BYOD policy (for example, acceptable uses, responsibilities); create training materials; consider implementing MDM software to manage mobile devices that connect to the corporate network; use compartmentalization/containerization by partitioning devices; create storage and retention policies; use encryption for devices and communications; address patch and software vulnerabilities; manage apps (list approved apps, and have a policy and procedure to manage how apps should be installed, updated, and removed); use safe authentication practices for devices, containers/compartments, and users; use malware protection; and create an incident management process.

[1235] *Maxam Bulk Services*, *supra* note 1088 at para 135.

[1236] *Ibid.*

[1237] *Ibid* at para 86.

[1238] *Ibid* at paras 184–189, 192–196.

That is, Lebrun did not even know whether his posts were public or private—the arbitrator protected Lebrun on the privacy issue, by downplaying the nature of the rants, even though Lebrun did not responsibly check his privacy settings before engaging in the online ranting.[1239] Instead, the arbitrator highlighted that there was a low risk of recurrence, and Lebrun's motivation involved believing that Maxam was being blamed for the sheep deaths.[1240] The arbitrator treated Lebrun with dignity by extending him the safety that he needed in order to express his frustrations with friends online; this, together with the lack of a company policy stipulating the expectations regarding online behaviour, enabled the arbitrator to give Lebrun the benefit of the doubt and the understanding that he required during the arbitration.[1241]

I have just examined the arbitrator's application of the dignity/human rights approach to privacy. The third thing that I will do is discuss some employment principles that applied in this case, such as a thorough balancing of aggravating and mitigating factors, progressive discipline, and the test for discipline when there has been off-duty misconduct.

To this end, there were some employment principles that played a critical role during this decision. More precisely, the arbitrator engaged in a thorough balancing of aggravating and mitigating factors, and methodically went through each factor before concluding that the balance tipped in favour of Lebrun.[1242] The arbitrator pointed out that the employment relationship was still viable, and an essential factor in the decision was that he believed that Lebrun learned his lesson and would conduct himself as the good and reliable employee that he was before his misconduct.[1243] The arbitrator noted that he was giving Lebrun the benefit of the doubt when attempting to understand the situation from his perspective.[1244] In particular, the arbitrator acknowledged Lebrun's attempts to apologize, show his remorse, explain that his motivations were not to compromise Maxam, and

---

[1239] *Ibid.*
[1240] *Ibid* at paras 192–196.
[1241] Hicks, *supra* note 1129 at 16–17.
[1242] *Maxam Bulk Services*, *supra* note 1088 at paras 140–202.
[1243] *Ibid* at paras 198–199.
[1244] *Ibid.*

promise that he would not repeat his behaviour.[1245] The arbitrator used a humane approach and allowed Lebrun to explain his side of the story when discerning the relevant mitigating factors.[1246]

In the same way, the employment principle of progressive discipline was vital in this case, because the arbitrator opined that Lebrun was a good candidate for the benefit of corrective discipline, something that had not yet been used with Lebrun.[1247] The arbitrator emphasized the importance of continued employment in light of the circumstances.[1248]

The doctrine of progressive discipline involves a system where an employer applies discipline for relatively minor infractions and misconduct on a progressive basis or in a series of steps; each step has a progressively more severe penalty until the final step, which is dismissal.[1249] Employers typically use a progressive discipline policy that sets out various levels of discipline such as verbal warnings, written warnings, and suspensions, and ultimate discharge.[1250] Progressive discipline is a pronounced feature of unionized employments, and a corrective approach is used in the interest of fairness.[1251] In particular, the approach provides employees with the chance to improve performance and behaviour.[1252] Progressive discipline can also be used in nonunionized workplaces through the use of a progressive discipline policy.[1253] Also, progressive discipline policies communicate the governing standards to employees, and ensure that instances of misconduct are addressed in a uniform manner.[1254] Using such a policy sends a clear

---

[1245] *Ibid* at paras 173–175; Hicks, *supra* note 1129 at 16–17; *Alberta Reference*, *supra* note 1174 at para 95; *Steel Appeal*, *supra* note 1113 at para 11.
[1246] *Ibid*.
[1247] *Maxam Bulk Services*, *supra* note 1088 at paras 170, 173.
[1248] *Ibid* at paras 199–202.
[1249] *Airport Inn v Newfoundland Association of Public Employees* (1992), 1992 CarswellNfld 242 at paras 23−28, [1992] Nfld LAA No 61 (Arbitrator: Alcok); *United Steelworkers, Local 5795 and Iron Ore Company of Canada* (2015), 2015 CarswellNfld 343 at paras 41−42, 124 CLAS 184 (Arbitrator: Oakley); The Honourable Mr Justice Randall Scott Echlin & Christine M Thomlinson, *For Better or Worse: A Practical Guide to Canadian Employment Law*, 2nd ed (Aurora, Ontario: Canada Law Book, 2003) at 182.
[1250] Echlin & Thomlinson, *supra* note 1249 at 182.
[1251] Bueckert, *supra* note 1130 at 15.
[1252] *Ibid*.
[1253] Echlin & Thomlinson, *supra* note 1249 at 182.
[1254] *Ibid* at 182–183.

message that the employer does not condone the misconduct.[1255] By condonation, I do not mean approval of behaviour, but rather a situation where the employer is aware of the employee's misconduct, but does nothing to address it.[1256] Warnings given in line with the progressive discipline policy typically set out the performance or behavioural problem in detail, explain the standard that is expected of the employee, and list the actions that must be taken to improve.[1257] In cases where performance is an issue, the employer explains how much time that the employee has to improve, along with how and when the performance is to be reassessed.[1258] It is critical that employers clearly state (preferably in writing) what the consequences will be if the performance does not improve, and whether the warning constitutes a final warning.[1259]

Lastly, another important employment principle is the test for discipline when there has been off-duty misconduct, namely the test in *Millhaven Fibres*, which makes it possible to connect off-duty misconduct with the workplace and justify a dismissal. In this case, the arbitrator did not specifically go through each of the criteria in the test and decide whether one or more of the criteria were met; instead, the arbitrator went straight into weighing of the aggravating and mitigating factors, and considered all of the circumstances when determining whether Maxam's response was appropriate in light of those factors.[1260] The arbitrator also compared the case to similar Internet rants when making the decision at the end of the balancing process.[1261] In unionized workplaces, employers are typically unconcerned about how employees spend their time while they are off-duty, but they become very concerned once there is misconduct that could harm the employer's reputation or other business interests.[1262] Arbitrators determine whether the test in *Millhaven Fibres*, is met, where only one of the criteria needs to be met; yet as with each just cause case, the analysis involves considering all the circumstances and

---

[1255] *Ibid* at 183.
[1256] *Ibid* at 206.
[1257] *Ibid.*
[1258] *Ibid.*
[1259] *Ibid* at 183–184.
[1260] *Maxam Bulk Services, supra* note 1088 at paras 140–202.
[1261] *Ibid* at paras 184–196.
[1262] David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 1131 at 243.

balancing of the aggravating and mitigating factors.[1263] In unionized workplaces, employers must persuade an arbitrator that it had just cause to dismiss the employee.[1264] In this case for example, Maxam could not show just cause to dismiss Lebrun.

In contrast, in nonunionized workplaces, employers must provide notice when dismissing, or they must be able to show that there was cause for summary dismissal.[1265] In off-duty misconduct situations involving social media, an employer must show that there is a nexus or connection between the employee's behaviour and prejudice to the employer's business interests, which can include economic interests, ability to have trust and confidence in the employee, or ensure there is not a poisoned work environment.[1266] Dismissals for just cause involve situations where the employee has engaged in conduct that constitutes a breach of the employee's fundamental obligations to the employer, or is incompatible with the faithful carrying out of the employee's duties to the employer, and where employers can terminate the employment relationship without providing notice.[1267] An on-duty nonunionized example would be *Steel*, where it was found that Coast had just cause to terminate Steel.

In this part, I extracted principles and values from *Maxam Bulk Services*. I accomplished this goal by pointing out the importance of having a social media policy, using a dignity/human rights approach to privacy, and applying some important employment principles such as balancing mitigating and aggravating factors, progressive discipline, and using the test for discipline involving off-duty conduct.

5.2.3 Implications for the New Workplace Privacy Regime

What the foregoing suggests is that it is essential for employers to have social media policies. Hence, I argue that there needs to be provisions requiring the creation of these policies that explain the public nature of social media, the realities of the online environment, and how ubiquitous surveillance can be used to aggregate their information

---

[1263] *Ibid* at 243−244.
[1264] *Ibid* at 231.
[1265] *Ibid.*
[1266] David Doorey, "Common Law and Regulation", *supra* note 1131 at 179−180.
[1267] Echlin & Thomlinson, *supra* note 1249 at 203.

in ways that can harm employees, the employer, or the employer's clients. This involves requiring employers to set out their expectations regarding social media use inside and outside the workplace, especially regarding choice of language when they are posting as a representative of the employer. This involves having a provision that requires employers to explain the consequences for noncompliance, taking into consideration crucial employment principles such as progressive discipline.

5.3 *Graphic Packaging*

The first American workplace privacy case that is discussed in this dissertation is *Graphic Packaging.* I first describe the facts and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.3.1 The Facts and Decision

The employee, who I will call "T", had worked as a press operator with his employer, Graphic Packaging International, Inc (Graphic Packaging), for 34 years.[1268] Following a work injury, he reported additional unresolved issues regarding his left shoulder and left lower back.[1269] He was diagnosed with a lumbar strain and a left shoulder strain, and was referred to a chiropractor.[1270] However, this led to further pain in his left leg, so he stopped the treatment, had an MRI, and was put on "seated work only" by his doctor.[1271] While he took time off in the form of vacation days and personal days, his doctor put him on different work restrictions, namely lifting only up to five pounds, pushing or pulling up to five pounds with the left side, and no work above the shoulder level with the left arm; Graphic Packaging had no such work at the time.[1272]

T was involved in an unrelated family dispute, where T and his neighbours, his mother and sister, were involved in a property line boundary dispute that caused T to hammer in

---

[1268] *Graphic Packaging*, *supra* note 1089 at 369.
[1269] *Ibid* at 370.
[1270] *Ibid.*
[1271] *Ibid.*
[1272] *Ibid.*

some stakes into the ground and used connecting rope to denote the line.[1273] Not only did T's sister call the police, but she, as a former employee of Graphic Packaging, also called Graphic Packaging and stated that T had been hammering in stakes and violating his medical restrictions regarding his workers' compensation.[1274] The HR manager at Graphic Packaging then contacted a private investigator, who conducted video surveillance on T for a couple of days, took some photographs, and sent reports along with the police incident report containing photos of the stakes.[1275] The video taken by the private investigator lasted a few minutes and showed T washing his car, and potentially using his arm in violation of his work restrictions; moreover, when stepping up into the car, he appeared to be pulling himself up using his left arm.[1276] The HR manager emailed the surveillance information to the doctor and asked for his medical opinion on whether T was acting outside his work restrictions.[1277] The doctor stated that when T hammered the stakes or pulled himself up in the car, he was performing activities that were outside his restrictions, and there were other activities where he could not make a determination.[1278]

However, even before receiving the doctor's email response, and before communicating with T on the issue, Graphic Packaging decided to terminate T.[1279] The HR manager phoned the union steward and asked him to come to her office to discuss discipline for T, and when the union steward arrived, she called T at home.[1280] When T did not answer the phone, the HR manager left a voice message telling him that he was dismissed, and to call her if he had any questions.[1281] The termination letter dated the next day stated that T was fraudulent when he made the workers' compensation claim.[1282] About four weeks after this letter was sent, Graphic Packaging sent another letter, this time stating that the previous termination letter contained a scrivener's error—the new letter stated that T was

---

[1273] *Ibid.*
[1274] *Ibid.*
[1275] *Ibid* at 370–371.
[1276] *Ibid* at 371.
[1277] *Ibid.*
[1278] *Ibid* at 372.
[1279] *Ibid.*
[1280] *Ibid.*
[1281] *Ibid.*
[1282] *Ibid.*

dismissed for falsifying the restrictions that formed the basis of his unpaid leave of absence, and not for filing fraudulent workers' compensation claim.[1283]

T launched a grievance and asserted that he was unjustly dismissed, and requested reinstatement; a meeting was supposed to take place during the grievance process, but the HR manager told the union steward that the company did not want T to be on company grounds and he could not attend the meeting.[1284] During the meeting, the union steward asked why T was dismissed, and the union was directed to the videotape, where Graphic Packaging suggested that the tape spoke for itself: "Well, you seen the tape, you know".[1285] The union asked why Graphic Packaging did not like T, and the response was, "Well, you know he's not very well liked", and the HR manager added that T gave false information to the doctors.[1286]

At the grievance, Graphic Packaging argued that there was just cause for the dismissal because T was aware of the company Code of Conduct and Ethics, and the possibility of discharge for violations.[1287] Graphic Packaging insisted that it properly notified the union of the disciplinary action pursuant to Article 25 of the collective bargaining agreement, and even had a union steward present during the phone call to T.[1288] This was a clear case of falsifying medical restrictions.[1289] On the other hand, the union argued that Graphic Packaging committed egregious violations of basic procedural fairness by not giving T an adequate opportunity to present his side of the story before being discharged, and by changing the reason for the discharge as seen in the two termination letters.[1290] Also, there was no evidence to support the allegations of falsification of restrictions.[1291]

The arbitrator, Wolff, decided that, while the collective bargaining agreement did have a discussion on discharge for just cause, T was denied due process twice because he could

---

[1283] *Ibid.*
[1284] *Ibid.*
[1285] *Ibid* at 373.
[1286] *Ibid.*
[1287] *Ibid* at 373–374.
[1288] *Ibid* at 374.
[1289] *Ibid* at 375.
[1290] *Ibid* at 375–376.
[1291] *Ibid* at 375–377.

not attend the meeting and be heard before being dismissed, and the reason for dismissal was changed in the second termination letter.[1292] Also, Graphic Packaging could not prove that there was any falsifying of medical restrictions.[1293] Essentially, Graphic Packaging accused T of committing fraud without even calling the doctor as a witness in the hearing.[1294] The arbitrator also found that neither the videos nor the doctor's responses proved that T exceeded the restrictions.[1295] The arbitrator reinstated T and also awarded special remedies including reimbursement for medical bills and explaining to any creditor that T was without fault in any delay of payments because of the improper discharge.[1296] And since T had difficulty refinancing his home because of this incident and experienced higher interest rates due to the loss of refinancing, the arbitrator remanded this issue to the parties to resolve on their own, or else they would have to return the issue to the arbitrator within 60 days.[1297]

5.3.2 Analysis of *Graphic Packaging*

This case involved the following features of workplace privacy cases: T was successful in being reinstated; the matter involved a labour arbitration; the surveillance scenario dealt with proactive surveillance operations; the electronic surveillance technology involved photographs and covert video surveillance using the private investigator's video camera; and the conduct took place while the employee was off-duty.

My goal in this section is to extract principles and values from *Graphic Packaging*. First, I will highlight the considerable abuse of surveillance power present in this case. Second, I will discuss employment principles that applied such as procedural fairness and also the absence of certain policies and procedures or clauses in the collective agreement to address electronic surveillance and privacy concerns. And third, I will examine the significance of further employment principles involving the impact of particular clauses in the collective bargaining agreement as well as policies and procedures.

[1292] *Ibid* at 378.
[1293] *Ibid* at 379.
[1294] *Ibid.*
[1295] *Ibid* at 379–380.
[1296] *Ibid.*
[1297] *Ibid.*

Thus, the first thing to point out in this case was Graphic Packaging's unquestionable abuse of surveillance power. Based on what was discovered after T's sister called and notified Graphic Packaging that T hammered in some stakes into the ground, involving photographs and a few minutes of video footage by the private investigator showing T washing his car (where he was not exceeding any restrictions after all), the HR manager promptly emailed T's doctor for an opinion about whether the activities fell outside T's medical restrictions.[1298] It was almost as if Graphic Packaging was looking for a reason to get rid of T, and the photographs and video footage could constitute a credible rationale.

Even worse, it appeared as though Graphic Packaging automatically assumed that, since there existed photos and video footage, there was indeed proof of misconduct; correspondingly, since T's sister called with the information, it was accepted as proof of wrongdoing without a great deal of probing on Graphic Packaging's part as to the source of the information or the context of T's hammering activities.[1299] What transpired was a quick dismissal by phone and a meeting, which T was not allowed to attend, where Graphic Packaging admitted that T was not well liked and suggested that the surveillance information spoke for itself to justify the dismissal.[1300] Graphic Packaging did not even scrutinize the surveillance information, wait for the opinion of the doctor, or discuss the issue with T before deciding to terminate T.[1301]

The most troubling aspect occurred when, after interpreting the surveillance information, Graphic Packaging acted inappropriately by terminating T, an employee who had been working with the company for 34 years, by phone message during a meeting that he was not allowed to attend.[1302] Graphic Packaging's mishandling of the situation did not go unnoticed by the arbitrator; in fact, T was reinstated, and was entitled to receive special remedies because of the improper discharge.[1303]

[1298] *Ibid* at 370–371, 379–380.
[1299] *Ibid*.
[1300] *Ibid* at 373.
[1301] *Ibid* at 372.
[1302] *Ibid* at 369, 372, 375–376.
[1303] *Ibid* at 380.

Beyond a doubt, this case was an example of an employer using electronic surveillance in a manner that went too far, and the level of intrusiveness drove T directly into the Panopticon and forced him to be subject to Graphic Packaging's gaze in two respects: first, T was exposed by the photos, in the police report due to the notification by his sister and also photos by the private investigator, and second, T was subjected to additional illumination with the video footage from the private investigator.[1304] Though Graphic Packaging argued that it was common for employers to conduct surveillance in a workers' compensation claim and to obtain doctors' opinions about employees exceeding their restrictions,[1305] in my view, Graphic Packaging's actions went beyond what would be considered necessary or reasonable.

Surely, it is understandable why employers would wish to overuse panoptic power and rapidly make decisions that affect employees' ability to earn a living without delving deeply into the matter; managers face pressures, and the act of increasing visibility and transparency reduces the amount of effort that is required compared to the exertion that is necessary to maintain reciprocal employment relationships.[1306] However, using the techniques of control and panoptic power limits what can be learned in the critical window of time prior to making a disciplinary decision, and does not contain the same quality as face-to-face interactions; in this case, it may have been helpful for Graphic Packaging to first talk to T before rashly jumping to the several conclusions that led to his hasty dismissal.[1307]

This is why it is necessary to have protections in place for employees so they can be treated as ends in themselves rather than means to furthering some other goal; in order to protect the dignity and self-respect of employees, it is important to have policies and

---

[1304] Michel Foucault, *Power/Knowledge: Selected Interviews & Other Writings 1972–1977*, edited by Colin Gordon, translated by Colin Gordon et al (New York: Vintage Books, 1980) at 147, 154–155 [Michel Foucault, "Power/Knowledge"]; Torin Monahan & David Murakami Wood, "Society and Subjectivity" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) at 28; *Graphic Packaging*, *supra* note 1089 at 370–371.
[1305] *Graphic Packaging*, *supra* note 1089 at 374.
[1306] Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York: Basic Books, 1988) at 323 [Shoshana Zuboff, "Smart Machine"].
[1307] *Ibid*.

procedures in place to prevent this mistreatment of an employee who was "not well liked".[1308] Clearly, some employees are more vulnerable than others because they are not the most popular employees in the workplace—since all employees are equally worthy by virtue of being human, these individuals need to be treated with dignity and respect in order to prevent the abuse of surveillance power and the targeting strategies aimed at justifying dismissals.[1309] I would like to suggest that one way to achieve this goal is to have proper policies and procedures in place with respect to deciding when and how to commence conducting electronic surveillance, increase levels of intrusiveness, interpret surveillance evidence, cease surveillance activities, and make disciplinary decisions based on electronic surveillance evidence.

I have therefore underscored the abuse of surveillance power that was present in this case and its ramifications. The second thing that I will do is consider the arbitrator's reliance on important employment principles when deciding the case, such as procedural fairness, and also the absence of certain policies and procedures or clauses in the collective agreement to address electronic surveillance and privacy concerns.

More precisely, the main principle that the arbitrator relied upon was procedural fairness, given that T was denied due process twice with respect to attending the meeting and the two different reasons for the dismissal.[1310] With respect to procedure, in the labour arbitration process, there is a grievance procedure that must be followed.[1311] The first step in the process involves filing a grievance, which triggers the legal process that is outlined in the collective bargaining agreement's grievance procedure.[1312] With individual grievances, employees file the grievance and make an allegation that a collective bargaining right has been violated by the employer.[1313] The employee would subsequently provide information relating to the alleged breach of the collective

---

[1308] *Ibid* at 373; Chris D L Hunt, "Conceptualizing Privacy and Elucidating Its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2001) 37 Queen's LJ 167 at 203−204; *Alberta Reference*, *supra* note 1174 at para 95.
[1309] George Kateb, *Human Dignity* (Cambridge: Harvard University Press, 2011) at 5–9.
[1310] *Graphic Packaging*, *supra* note 1089 at 378.
[1311] David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 1131 at 214.
[1312] *Ibid.*
[1313] *Ibid.*

bargaining agreement and indicate what remedy is being sought.[1314] The employer would be required to respond within a certain period of time as set out in the grievance procedure.[1315] Where the employer accepts the grievance, there is a grievance settlement; where the employer denies the grievance, the grievance proceeds to the next stage in the grievance procedure.[1316] At this point, there are a series of meetings that take place in order to attempt to arrive at a settlement between the parties.[1317] In cases where a settlement is reached, the grievance is withdrawn and a settlement agreement is created.[1318] Otherwise, the matter proceeds to arbitration.[1319] The union decides whether the settle, withdraw, or refer the matter to arbitration.[1320] After the arbitration, the labour arbitrator writes a decision that explains the reasoning and sets out the remedy.[1321] The decision is final and binding on the parties who are affected; although it is not binding in the sense that it creates precedent as with courts, it becomes part of the labour arbitration decisions that are referenced by parties during labour disputes.[1322]

Another thing that the arbitrator could have examined more thoroughly was whether Graphic Packaging violated T's privacy in light of the surveillance that was conducted on T, but there appeared to be no workplace policies and procedures or clauses in the collective agreement specifically dealing with surveillance or privacy for the arbitrator to examine. Also, the arbitrator did not hesitate to admit the photographs and video footage into the hearing as evidence, and simply proceeded to focus on the violations of procedural fairness.[1323] Indeed, the arbitrator used the standard of relevance to admit and examine the surveillance evidence; this involves admitting the evidence if it is relevant and probative, similar to the approach taken by courts.[1324]

[1314] *Ibid* at 215.
[1315] *Ibid.*
[1316] *Ibid*.
[1317] *Ibid.*
[1318] *Ibid* at 216−217.
[1319] *Ibid* at 215.
[1320] *Ibid* at 218.
[1321] *Ibid* at 220.
[1322] *Ibid* at 219−220.
[1323] *Graphic Packaging, supra* note 1089 at 378−380.
[1324] Bueckert, *supra* note 1130 at 110−118. American arbitrators take a flexible approach towards the admission of evidence such that in the majority of cases, any evidence, information, or testimony is

Given the lack of privacy protections in place in the workplace documents, T's only option was to insist that there had been procedural infractions, and rely on the surveillance evidence to show that there were no violations of his medical restrictions.[1325]

I have just examined some of employment principles such as procedural fairness and noted the absence of protections in the workplace documents. The third thing that I will do is point to some further employment principles, such as the impact of particular clauses in the collective bargaining agreement along with company policies and procedures.

More precisely, regarding management rights involving disciplinary decisions, the collective bargaining agreement required Graphic Packaging to notify the union in writing immediately if possible, but no later than within two days, of the employee's offence, and also the action that was taken by Graphic Packaging in response.[1326] Furthermore, Graphic Packaging had a Code of Conduct and Ethics, and T was aware that he could be dismissed for violating it.[1327] In fact, the arbitrator looked to the collective bargaining agreement and concluded that there was a discussion about discharges for just cause.[1328]

---

admitted if it is pertinent to the case and if it helps to understand and decide the problem. See Elkouri & Elkouri, *How Arbitration Works*, 8th ed, Bloomberg BNA, (Chicago: American Bar Association, 2017) at 8–7 (BNA). In Canada, the question on admissibility of evidence has been more controversial among labour arbitrators. In addition to the relevance test, some arbitrators choose to use a two-part reasonableness test when examining video-surveillance, asking (1) whether it was reasonable to request surveillance, and (2) whether the surveillance was conducted in a reasonable manner. Indeed, there are divergent approaches on the issue in Canada; recent decisions have confirmed that arbitrators have the jurisdiction to refuse to admit relevant evidence (such as video surveillance evidence), as long as in doing so it does not result in a denial of natural justice, and tend to favour the 2-part reasonableness test. See *The Toronto Transit Commission and The Amalgamated Transit Union, Local 113* (2019), 2019 CarswellOnt 3593 at paras 80−83, 91, 301 LAC (4th) 1 (Arbitrator: Johnston). The law of admissibility of evidence is outside the scope of this dissertation. The purpose of this dissertation is to close the electronic surveillance gap in employment by creating a new workplace privacy regime.

[1325] *Graphic Packaging*, *supra* note 1089 at 376–377.

[1326] *Ibid* at 374.

[1327] *Ibid* at 373–374, 378.

[1328] *Ibid* at 378.

It is important to appreciate that the collective bargaining agreement is an important document in unionized workplaces because the jurisdiction of labour arbitrators comes from the collective agreement.[1329] Not only does the collective agreement contain the grievance procedures as noted above, but it enables the creation of rules and policies that affect privacy and other relevant workplace issues that pertain to the workplace; there is no single set of rules or policies, and they differ depending on the circumstances of each bargaining situation between the particular parties.[1330]

The creation of rules and policies is considered to be an inherent right of management, unless this right is taken away by the terms of the collective agreement.[1331] Workplace rules and policies are created in one of two ways; the first way is through an agreement between the parties, and the second way is through the unilateral imposition of rules and policies by the employer.[1332] Firstly, when the parties agree, the rule or policy is typically attached to the collective agreement by way of an appendix, for example, and then it becomes clear that the rule or policy must be followed.[1333] In this situation, arbitrators do not interfere with penalties imposed by employers in accordance with those rules that are jointly agreed to by the parties.[1334] Secondly, when the employer unilaterally imposes a rule or policy, there is a concern that the rule or policy may not be reasonable, and also that employees may not be aware of the rule or policy; this could be problematic in cases where employees are dismissed for failing to follow unreasonable rules, or rules they were not aware of.[1335] To that end, rules or policies that are unilaterally imposed by the employer must: (1) not be inconsistent with the collective agreement; (2) not be unreasonable; (3) be clear and unequivocal; (4) be brought to the attention of the employee affected before the employer can act on them; (5) be known in that the employee was notified that a breach of such rule could result in discharge; and (6) have

---

[1329] Bueckert, *supra* note 1130 at 13.
[1330] Mitchnick & Etherington *supra* note 1133 at 393–415.
[1331] *Lumber & Sawmill Workers' Union, Local 2537 v KVP Co* (1965), 1965 CarswellOnt 618 at para 17, [1965] OLAA No 2 (Arbitrators: Wren, Robinson & Hicks) [*KVP*].
[1332] Bueckert, *supra* note 1130 at 17.
[1333] *KVP*, *supra* note 1331 at para 20.
[1334] *Ibid* at para 23.
[1335] *Ibid* at paras 23−32.

been consistently enforced by the employer from the time that it was introduced.[1336] Where there is a dismissal because of a breach, and the breach forms the basis for the discharge, the employer would still have to show that there was just cause for the dismissal, since the very issue before the arbitrator may involve determining the reasonableness of the rule or policy.[1337] When assessing the reasonableness of a rule or policy that is unilaterally imposed, arbitrators use the "KVP Test"[1338] that has the six factors mentioned above; the heart of the test involves asking whether the rule or policy was consistent with the collective agreement and reasonable; arbitrators perform a balancing of the interests of the employer and the employee.[1339]

Where the collective agreement expressly refers to an issue so as to bring the subject matter within the scope of the collective agreement, the arbitrator has the jurisdiction to decide whether the employer has complied with the terms, keeping in mind the limits of the arbitrator, who is charged with settling disputes arising out of the interpretation, application, administration, or alleged violation of the collective agreement.[1340] Regarding issues such as privacy, arbitrators look to the collective agreement, and where it is silent, they balance the interests of the parties.[1341]

In this case, I would like to suggest that but for the procedural infractions regarding T's disciplinary proceedings, T would not have been adequately protected against the abuse of electronic surveillance power, because there were simply no protections in place on examination of the company rules, policies, procedures, or the collective agreement.[1342] Indeed, many employers lack specific policy provisions, and there is also a corresponding lack of awareness of monitoring policies and practices among employees; this situation

---

[1336] *Ibid* at para 34.
[1337] *Ibid* at para 35; Mitchnick & Etherington *supra* note 1133 at 393–395.
[1338] *Irving Pulp & Paper Ltd. v Communications, Energy and Paperworkers Union of Canada, Local 3027,* 2013 SCC 34 at para 24 [*Irving*].
[1339] *Ibid* at paras 24−27, 81−82
[1340] Donald J M Brown, QC & David Beatty, *Canadian Labour Arbitration*, 4th ed, vol 1 (Toronto: Thomson Reuters Canada Limited, 2017) at 2–7.
[1341] Mitchnick & Etherington *supra* note 1133 at 398, 403.
[1342] *Graphic Packaging, supra* note 1089 at 374–378.

crates a problematic hole that needs filling with the creation of basic protections.[1343] This is why it is necessary to establish a floor of fair protections and boundaries for all parties in all employment relationships, so there can be more even and sufficient protection of employees' dignity, while also balancing employers' legitimate business interests.[1344]

In this part, I extracted principles and values from *Graphic Packaging*. I achieved this by stressing the considerable abuse of surveillance power present in this case, and examining several employment principles such as procedural fairness, the absence of certain policies and procedures or clauses in the collective agreement to address electronic surveillance and privacy concerns, and the impact of particular clauses in the collective bargaining agreement as well as policies and procedures.

5.3.3 Implications for the New Workplace Privacy Regime

The previous analysis highlights the serious problem of the abuse of surveillance power. Employers are in a the more dominant position and have the potential to hastily order electronic surveillance of an employee, interpret surveillance information, and make swift disciplinary decisions that can harm employees. It is therefore necessary to have provisions in place that prevent the abuse of electronic surveillance power, including provisions requiring employers to respect the human dignity of employees by giving them the benefit of doubt and attempting to understand their version of the story before hastily commencing electronic surveillance, interpreting electronic surveillance reports, or acting upon any electronic surveillance information. It is also important to ensure that employers respect applicable policies and procedures, and contracts or collective agreements, when acting in good faith with employees. Another example could be adding a provision requiring employers to explain what is meant by suspicion in their policies and procedures for the purposes of deciding whether it is appropriate to conduct electronic surveillance of employees in the first place. There also needs to be clear

---

[1343] Kirstie Ball, "Workplace Surveillance: An Overview" (2010) 51:1 Labor History 87 at 89, online (pdf): *tandfonline* <www.tandfonline.com> DOI: <10.1080/00236561003654776> [Kirstie Ball, "An Overview"].
[1344] Kateb, *supra* note 1309 at 5–9; *Alberta Reference*, *supra* note 1174 at para 95.

boundaries within which employers can operate when deciding to conduct electronic surveillance of employees while they are off-duty.

5.4 *Baker Hughes*

The second American workplace privacy case that is discussed in this dissertation is *Baker Hughes.* I first describe the facts and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.4.1 The Facts and Decision

The employee, who I will call "G", worked as a machinery mechanic with his employer, Baker Hughes Inc (Baker Hughes), an industrial service company, for 29 years.[1345] The plant manager, who I will call "H", conducted a plant communications meeting with employees to discuss critical safety violations and to emphasize that violations could result in discharge.[1346] G was at the meeting, and when H was reading the rules line by line, G became angry and frustrated by the information that was being presented.[1347] The next day, H approached the HR Representative and mentioned that he discovered that G posted a blog on his MySpace account which contained discriminatory comments that were directed at H.[1348] More specifically, G made racist comments criticizing someone in upper management at the plant, and H was shocked and concerned about the contents; it was clear that the message was directed at H since he was the only person in upper management belonging to the targeted group.[1349] In a meeting with the HR Representative, G admitted that it was his blog on the website, and it was aimed at H; ultimately, G was dismissed.[1350] In response, G launched a grievance.[1351]

[1345] *Baker Hughes, supra* note 1090 at 37.
[1346] *Ibid* at 37–38.
[1347] *Ibid* at 38.
[1348] *Ibid.*
[1349] *Ibid.*
[1350] *Ibid*
[1351] *Ibid.*

At the grievance, Baker Hughes argued that there was just cause for the dismissal because G violated the company policies, of which he was aware.[1352] The company rules were reasonable, and the discipline was reasonable in the circumstances since G's off-duty conduct created a hostile work environment sufficient to establish a claim of harassment.[1353] Baker Hughes asserted that G's misconduct had a nexus to the workplace, and G continued to disparage the plant management even after his discharge.[1354] On the other hand, the union argued that there was no just cause for the dismissal, since there was no company work rule prohibiting inappropriate use of one's personal computer at home, the comments were made while G was off-duty, and the remarks were not sent to or retrieved from a company computer.[1355] That is, since the Anti-Harassment Policy only applied on company premises, it did not apply in this case.[1356] G also claimed that he believed that his blog was a private account open only to friends.[1357]

The arbitrator, Baroni, reviewed the provisions of the collective agreement and noted that there were clauses prohibiting discrimination against an individual because of race, colour, national origin, sex, or age.[1358] Additionally, the non-discrimination clause had a specific reference to the *Civil Rights Act*.[1359] Moreover, the arbitrator noted the company Anti-Harassment Policy that prohibited discrimination and harassment of any type in the working environment, encouraged mutual respect, and promoted respectful and congenial relationships between employees.[1360] It applied to everyone in the workplace, including supervisors, coworkers, or non-employees who engaged in verbally or physically harassing behaviour that had the potential to be humiliating or embarrassing.[1361] Also, the Plant Rules prohibited insubordination and any form of harassment.[1362]

[1352] *Ibid* at 39.
[1353] *Ibid.*
[1354] *Ibid.*
[1355] *Ibid.*
[1356] *Ibid.*
[1357] *Ibid* at 42.
[1358] *Ibid*.
[1359] *Civil Rights Act of 1964 Pub L*, 88–352, 78 Stat 241, §§ 2000e-2(a) [*Civil Rights Act*].
[1360] *Baker Hughes, supra* note 1090 at 38–39.
[1361] *Ibid.*
[1362] *Ibid.*

The arbitrator concluded that there was a nexus between the misconduct and the workplace, and G's actions were captured by the company Anti-Harassment Policy even though he was engaging in off-duty conduct away from the company premises; he created a hostile work environment sufficient to establish a claim of harassment on the ground of national origin.[1363] The arbitrator also emphasized that protecting employees from harassment by coworkers was a legitimate business interest.[1364] The arbitrator recognized that insubordinate off-duty language directed at a supervisor could have long-lasting and harmful effects in the workplace; in this case, it could hurt H and also permanently disrupt the safe and efficient operations of the plant.[1365]

The arbitrator noted that employees were more frequently being "dooced", or dismissed from work because of employees' derogatory online postings about their employers.[1366] The arbitrator stated that the point of upholding such terminations was to establish a precedent of common sense and fairness in the workplace, and to make it clear that inappropriate commentary about coworkers on blogs was not immune from an appropriate response from employers.[1367] The arbitrator stated, "Character assassination is the same whether spoken to a crowd or posted on an Internet blog".[1368] The arbitrator also found that G opened his blog to the public when he ran for City Council.[1369] During the investigation, G was bragging about the size of his readership and claiming that everyone in town must have been reading his posts; he continued to leave the offensive language and racist slurs on his blog during the investigation and also after his dismissal, and it was not until right before the hearing that he changed the settings to private.[1370] The arbitrator concluded that the blog was public and not private as G claimed, and G caused harm to H's reputation and disrupted industrial harmony in the plant.[1371] Also, the arbitrator noted that G showed no remorse, did not apologize, and already had five forms

---

[1363] *Ibid* at 40.
[1364] *Ibid.*
[1365] *Ibid* at 41.
[1366] *Ibid.*
[1367] *Ibid.*
[1368] *Ibid.*
[1369] *Ibid* at 42.
[1370] *Ibid.*
[1371] *Ibid.*

of discipline on his record with a final warning.[1372] The arbitrator concluded that there was just cause for G's dismissal, and there could be no reinstatement in this case since that would send the wrong message in the workplace.[1373]

5.4.2 Analysis of *Baker Hughes*

This case involved the following features of workplace privacy cases: G's dismissal was upheld; the matter involved a labour arbitration; the surveillance scenario involved the discovery of employee misuse of technology; the electronic surveillance technology involved social media, namely blogs on MySpace; and the misconduct took place while G was off-duty.

One may question how this case was different than *Maxam Bulk Services.* In *Baker Hughes,* G made racist comments online, showed no remorse, offered no apology, had a prior disciplinary record, and violated clear company rules of which he was aware given his position in the company as a senior employee in a leadership role. Conversely, in *Maxam Bulk Services,* Lebrun was quite the opposite since, while he made inappropriate comments online that were filled with profanities, he was remorseful, he apologized, he was a good employee with no disciplinary record, he was mid-range in seniority, he was found to be just venting his frustrations, and there were no company policies prohibiting his misbehaviour. Both cases were decided by labour arbitrators, but the balance of interests tipped in opposite directions.

While both cases dealt with online misconduct by employees while they were off-duty, I believe that the outcomes were opposite for a few reasons. Firstly, one main difference involved the presence of a clear company policy. In *Maxam Bulk Services*, it remained unclear what the rules were regarding employees' social media use, and what the disciplinary consequences would be in cases of noncompliance. Yet in *Baker Hughes*, there were clear workplace policies and plant rules, and also clauses in the collective agreement, which prohibited insubordination and harassment of coworkers including

---

[1372] *Ibid.*
[1373] *Ibid.*

supervisors. The employer ensured that the employees were aware of the rules. The goal was not so much on protecting the employer's reputation or confidential information, but rather on protecting the employees in the workplace from harm and promote harmonious relations in the plant. Secondly, in *Maxam Bulk Services,* Lebrun nonchalantly used profanities on Facebook walls without checking privacy settings just to blow off some steam, and inadvertently harmed the reputation of his own employer, Maxam, along with that of Maxam's main client. The arbitrator took this lack of intention to injure Maxam or Teck into account when making the decision. In contrast, in *Baker Hughes*, the misconduct was more calculated, since G deliberately used a public blog to target a specific manager, and did so with malevolent intentions. The result was a disruption in the workplace because of G's destructive attack of H. Thirdly, in *Maxam Bulk Services,* Lebrun was remorseful and made efforts to apologize to Maxam and Teck; accordingly, the arbitrator could see the perceived potential for reinstatement and the continuation of harmonious employment relations. But in *Baker Hughes,* G kept his blog public until right before the hearing and never apologized to anyone. The situation was only made worse when considering G's disciplinary record. In this case, the arbitrator could see that reinstatement would send the wrong message in the workplace.

My goal in this section is to extract principles and values from *Baker Hughes*. First, I will address the question of the private versus public nature of the blog. Second, I will review the employment principles that applied such as policies and procedures, and also clauses in the collective agreement. And third, I will point to the legitimate business interests of employers to prevent employees from harassing coworkers in the workplace.

Therefore, the first thing to pay attention to in this case was the question about whether G's blog was private. More precisely, G argued that he believed that his MySpace account was a private account that was only open to friends.[1374] However, the arbitrator found this argument difficult to believe, especially since G opened his blog to the public when he ran for City Council, bragged about the size of his readership, and kept the offensive and racist comments on his blog after his dismissal up to and until right before

[1374] *Ibid*.

the hearing.[1375] Therefore, contrary to what G claimed, the arbitrator confirmed that G's MySpace account was clearly a public account.[1376]

In this situation, G appeared to be using more of an economic theoretical approach to privacy, where he viewed and treated privacy as something that could create opportunities for gain.[1377] In particular, G seemed to be under the impression that the process of voluntary exchange of personal information ensured that the information was put to its most valuable use, considering factors such as the nature and provenance of the information, and transaction costs.[1378] Indeed, G came across as an individual who wanted to manipulate the world around him by selective disclosure of facts about himself, and then turn around and claim that his privacy should be protected just at the moment when he needed to fight to keep his job.[1379] This had the unintended consequence of G not being taken seriously when he tried to make a convincing argument about his account being private.[1380] In fact, G was not viewed as credible and was not given the benefit of the doubt after exploiting his own information to further his political career, ego, and racist agenda, where he took advantage of the situation in the name of total utility.[1381]

This may be why G showed no remorse and did not apologize.[1382] Instead, G made targeted public comments aimed directly at H.[1383] For the sake of furthering fairness in the workplace, the arbitrator found that it was appropriate for G to be dooced as a result of his making derogatory online postings about H, in order to send the message that this misconduct was unacceptable.[1384]

[1375] *Ibid.*
[1376] *Ibid.*
[1377] Richard A Posner, "The Right of Privacy" (1977-1978) 12 Ga L Rev 393 at 394.
[1378] *Ibid.*
[1379] *Ibid* at 400; *Baker Hughes, supra* note 1090 at 42.
[1380] *Baker Hughes, supra* note 1090 at 42.
[1381] *Ibid*; James B Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" (2004) 54 U Toronto L J 183 at 85; Krister Bykvist, *Utilitarianism: A Guide for the Perplexed* (London: Continuum International Publishing Group, 2010) at 190.
[1382] *Baker Hughes, supra* note 1090 at 42.
[1383] *Ibid.*
[1384] *Ibid* at 41.

To be sure, this case was not one where an employee was exploited in a way that created a vector of vulnerability and a potential for the abuse of electronic surveillance power.[1385] This was certainly not a situation where G was controlled or manipulated for the purposes of shaping his behaviour using his exploited behavioural surplus.[1386] On the contrary, G was focussing only maximizing his own value and the value of his information for personal gain.[1387] In so doing, he injured H by threatening H's well-being, and compromised Baker Hughes by disrupting safe and efficient plant operations.[1388]

I have just addressed the question about whether the blog was public or private. The second thing that I will do is touch on the employment principles that applied in the decision, such as the examination of key workplace documents.

For example, the arbitrator spent a considerable amount of time examining the relevant provisions in the collective agreement, company Anti-Harassment Policy, and the Plant Rules.[1389] The arbitrator noted that there was a specific reference to the *Civil Rights Act* and discussed how it was becoming more common for employers to incorporate these types of principles directly into their policies and work rules.[1390] The arbitrator also confirmed that Baker Hughes had the right to create reasonable work rules so long as they were to be posted, distributed, and made known to all employees.[1391]

This close investigation of the key workplace documents enabled the arbitrator to make a decision as to whether the misconduct fell under the scope of these provisions, and whether there was a nexus between the off-duty online comments and the workplace.[1392] This was important since G argued that there was no company work rule prohibiting

---

[1385] Mark Andrejevic, "Automating Surveillance", *supra* note 1223 at 7–9.
[1386] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" in Torin & Wood, *supra* note 1304 at 279 [Christian Fuchs, "Web 2.0"]; Christian Fuchs, "Political Economy and Surveillance Theory" (2012) 39:5 Crit Sociology 671 at 685, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1177/0896920511435710> [Christian Fuchs, "Political Economy"]; Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019) at 52–53, 97 [Shoshana Zuboff, "Surveillance Capitalism"].
[1387] Rule, *supra* note 1381 at 185.
[1388] *Baker Hughes, supra* note 1090 at 41.
[1389] *Ibid* at 38–39.
[1390] *Ibid.*
[1391] *Ibid*.
[1392] *Ibid* at 38–40.

inappropriate use of one's personal computer at home, and since the comments were made while G was off-duty and the remarks were not sent to or retrieved from a company computer, the workplace policies and rules did not apply.[1393] In this case, the arbitrator decided that G violated the rules and created a hostile work environment sufficient to establish a claim of harassment on the ground of national origin.[1394] The arbitrator also confirmed that G's insubordinate off-duty language defied the rules, of which he was aware.[1395]

While the workplace documents were effective in capturing the type of misconduct that took place in this case because the misconduct was easily connected to workplace rules setting standards for the working environment, I would like to suggest that a more compelling way to tackle the issue of preventing online harassment of coworkers would be to create explicit policies and procedures that expressly prohibit *online* harassment and discrimination of coworkers contrary to the *Canadian Human Rights Act*.[1396] In this way, the message would more efficiently be sent to employees that the misconduct that is carried out in an online environment is just as unacceptable as when it is executed offline, and the disciplinary consequences of online harassment carry the same weight.

I have therefore shown the impact of examining core workplace documents during a decision. The third thing that I will do is note the arbitrator's emphasis of a key aspect of employers' obligations—the arbitrator confirmed that protecting employees from harassment by coworkers constituted a legitimate business interest.[1397]

The arbitrator concluded that this responsibility stemmed from the fact that it was harmful for employees to be subjected to demeaning and degrading behaviour, the effects

---

[1393] *Ibid* at 39.
[1394] *Ibid* at 40.
[1395] *Ibid* at 41.
[1396] *Canadian Human Rights Act*, RSC, 1985, c H-6, s 3 [*Canadian Human Rights Act*]. I assert that the most efficient way to address online harassment of coworkers is to create an express prohibition in company policies and procedures that specifically refers to the legislation.
[1397] *Baker Hughes*, *supra* note 1090 at 40.

could be long-lasting and affect a person's well-being, and the misconduct could wreak havoc on the plant's operations.[1398]

By extension then, one can deduce that protecting employees from online harassment by coworkers similarly constitutes a legitimate business interest for employers.

In this case, the focus was not on applying the dignity/human rights approach to privacy to protect the employee, G, who made racist comments on his MySpace account; rather, the priority was placed more so on protecting the dignity and self-respect of H, the manager who was harassed on the ground of national origin, by dismissing G.[1399] Put another way, the focus in this case was on protecting H's inherent value and worth.[1400] When societal values were balanced, the scale was tipped in favour of protecting Baker Hughes' legitimate business interests of protecting its employees from being harassed by coworkers. To that end, I would like to suggest that it is crucial for employers to be as clear as possible that there are certain expectations that employees need to respect when posting online.

In this part, I extracted principles and values from *Baker Hughes*. I executed this by addressing the question of the private versus public nature of the blog, discussing employment principles such as examining clauses in the collective agreement and policies and procedures, and arguing the benefits of recognizing the legitimate business interests of employers to prevent employees from harassing coworkers online.

5.4.3 Implications for the New Workplace Privacy Regime

What the prior analysis suggests is that employers have a legitimate business interest in protecting their employees from being harassed and discriminated against by coworkers. By extension, I argue that it is essential for employers to have social media policies that expressly prohibit the online discrimination or harassment of coworkers. Since the creation of comprehensive policies and procedures is critical, this can be accomplished

---

[1398] *Ibid* at 41.
[1399] *Alberta Reference*, *supra* note 1174 at para 95.
[1400] Hicks, *supra* note 1129 at 2.

by adding provisions that require employers to set out their expectations regarding acceptable online use, refer to existing workplace anti-discrimination and anti-harassment policies and procedures, and emphasize that it is not acceptable to harass or discriminate against coworkers online. There needs to be provisions requiring explanations in policies about the nature of the online environment and the public nature of blogs. To that end, I propose that there should be a provision stressing the importance that, while employees may have and use social media accounts while they are off-duty, they can never disparage coworkers and then use as an excuse that they were away from work or using their own digital devices.

5.5 *Bărbulescu*

The first European Union workplace privacy case that it is discussed in this dissertation is *Bărbulescu*. I first describe the facts, history, and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.5.1 The Facts, History, and Decision

The Romanian employee, Bogdan Mihai Bărbulescu (Bărbulescu), worked with his employer, a private company that I will call "E", for about three years as an engineer in charge of sales.[1401] E asked Bărbulescu to create a Yahoo! Messenger account for responding to client inquiries, and he complied with the request.[1402] E had Internal Regulations stating that it was strictly forbidden for employees to use computers, photocopiers, telephones, telex and fax machines for personal purposes.[1403] Bărbulescu was aware of this rule; E later circulated a notice to employees citing this rule and stressing that E had a duty to supervise and monitor employees' work, and take punitive measures against anyone at fault.[1404] The notice stated, "Your misconduct will be

---

[1401] *Bărbulescu v Romania*, Application 61496/08, Judgment of the Court (Fourth Section), 12 January 2016 at paras 1, 6 [*Bărbulescu Fourth Section*].
[1402] *Ibid* at para 6.
[1403] *Ibid* at para 8.
[1404] *Bărbulescu v Romania*, Application 61496/08, Judgment of the Court (Grand Chamber), 5 September 2017 at para 14−15 [*Bărbulescu Grand Chamber*].

carefully monitored and punished!"[1405] The notice referred to a coworker who disregarded these rules and was terminated.[1406] Bărbulescu was also aware of this notice and signed it, but it is not clear exactly when he did so.[1407]

After complying with E's request to create the account, Bărbulescu was later told that his communications had been monitored for eight days, and the records showed that he used the Internet for personal purposes contrary to the Internal Regulations.[1408] He responded by insisting that he had only used the account for professional purposes; yet, once he was shown the 45-page transcript of his communications, he asserted that E was violating criminal laws by intercepting his communications.[1409] The 45-page transcript contained messages that Bărbulescu exchanged with his fiancé and his brother, and some of the messages were personal in nature.[1410] E terminated Bărbulescu's employment for breach of the company's Internal Regulations.[1411]

When Bărbulescu challenged E's decision in the Bucharest County Court (County Court), and complained that E violated his rights protected by constitutional and criminal laws, he was unsuccessful.[1412] He appealed this decision to the Bucharest Court of Appeal (Court of Appeal), and argued that his communications were protected by Article 8 of the *EU Convention;*[1413] relying on the predecessor of the *GDPR*,[1414] the *Data Protection*

[1405] *Ibid* at para 15.
[1406] *Ibid.*
[1407] *Ibid* at paras 14−17. According to the Grand Chamber decision, Bărbulescu signed the notice sometime between July 3, 2007 and July 13, 2007. E monitored the communications at issue in real time from July 5, 2007 to July 13, 2007. Bărbulescu had been aware of the Internal Regulations since December 20, 2006.
[1408] *Bărbulescu Fourth Section, supra* note 1401 at para 7.
[1409] *Ibid*. An analysis of the domestic laws of European Union Member States is outside the scope of this dissertation. This discussion is confined to the European Union instruments.
[1410] *Bărbulescu Fourth Section*, *supra* note 1401 at para 7.
[1411] *Ibid* at para 8.
[1412] *Ibid* at paras 9−10, 13–14.
[1413] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5 (1950), art 8 [*EU Convention*].
[1414] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* [2016] OJ, L119/1 [*GDPR*].

Directive[1415] in force at the time, the Court of Appeal dismissed the appeal and confirmed that E's conduct was reasonable since monitoring the communications was the only way to establish that there had been a disciplinary breach.[1416] In response, Bărbulescu filed an application with the European Court of Human Rights, Fourth Section (Fourth Section),[1417] and argued that Romania violated Article 8 of the *EU Convention*[1418] because the domestic courts failed to protect his rights to private life and correspondence.[1419] He argued that his communications were private and fell within the scope of Article 8 of the *EU Convention*;[1420] also, he adamantly denied having been given proper notice of the monitoring, insisting that neither the Internal Regulations nor the notice to employees constituted proper prior notice of monitoring.[1421] The Fourth Section noted that it had to examine whether Romania, in the context of its positive obligations under Article 8 of the *EU Convention*,[1422] struck a fair balance between Bărbulescu's right to respect for his private life and correspondence, and E's legitimate business interests.[1423] The Fourth Section concluded that there was no violation of Article 8 of the *EU Convention*,[1424] since E acted within its disciplinary powers and accessed the Yahoo! Messenger account on the assumption that the information in question had been related to professional activities.[1425] Therefore, the Fourth Section concluded that it was reasonable for an employer to want to verify that the employees were completing their professional

---

[1415] EC, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] OJ, L281/0031at arts 3(a), 5(2)(a)(e), 5(3), 18(2) [*Data Protection Directive*].
[1416] *Bărbulescu Fourth Section, supra* note 1401 at para 12.
[1417] Ibid at para 1. The Chamber was composed of Vincent A. De Gaetano, Boštjan M Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Egidijus Kūris, Iulia Antoanella Motoc, judges, and Fatoş Aracı, *Deputy Section Registrar*.
[1418] *EU Convention, supra* note 1413 at art 8.
[1419] *Bărbulescu Fourth Section, supra* note 1401 at paras 1–3. In addition to the Article 8 argument, he argued that he was not able to make his arguments by calling witnesses in the domestic courts, contrary to Article 6 of the *EU Convention*. Article 6 of the *EU Convention* states that everyone is entitled to a fair hearing by a tribunal. The court disagreed with Bărbulescu and found that he was able to raise arguments, and hearing additional witnesses was not relevant to the case. See paras 64−66. A discussion of Article 6 of the *EU Convention* is outside the scope of this dissertation.
[1420] *EU Convention, supra* note 1413 at art 8.
[1421] *Bărbulescu Fourth Section, supra* note 1401 at para 33. The only notice filed with the court was dated July 3, 2007, and it was not signed.
[1422] *EU Convention, supra* note 1413 at art 8.
[1423] *Bărbulescu Fourth Section, supra* note 1401 at para 54.
[1424] *EU Convention, supra* note 1413 at art 8.
[1425] *Bărbulescu Fourth Section, supra* note 1401 at paras 57, 63.

tasks during work hours; since E only examined the communications on the Yahoo! Messenger account, and not the content or any other data stored on the computer, the monitoring was limited in scope and proportionate.[1426] Also, Bărbulescu could not explain why he used the Yahoo! Messenger account for personal reasons.[1427] Therefore, the domestic courts did not fail to strike a fair balance.[1428]

Bărbulescu appealed to the European Court of Human Rights, Grand Chamber (Grand Chamber).[1429] The Grand Chamber confirmed that the Internet instant messaging service was captured by Article 8 of the *EU Convention,*[1430] which guaranteed a right to private life and correspondence.[1431] Most importantly, the Grand Chamber emphasized that, although Bărbulescu had been informed of the ban on personal Internet use in the Internal Regulations, it was not so clear that he had been informed beforehand that monitoring of his communications was going to take place; he was certainly not informed about the nature and extent of the monitoring activity, or the possibility that E would be able to access the contents.[1432] The Grand Chamber stated:

> [A]n employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.[1433]

The Grand Chamber also noted that the employment relationship had special features to consider, and from a regulatory perspective, the law left room for negotiation between the parties regarding their employment contract; yet, the Grand Camber stated that the

---

[1426] *Ibid* at paras 58–60.
[1427] *Ibid* at para 61.
[1428] *Ibid* at paras 62–66.
[1429] *Bărbulescu Grand Chamber*, *supra* note 1404 at para 5. The Grand Chamber was composed of: Guido Raimondi, *President,* Angelika Nußberger, Mirjana Lazarova Trajkovska, *judges*, Luis López Guerra, ad hoc *judge*, Ledi Bianku, Işıl Karakaş, Nebojša Vučinić, André Potocki, Paul Lemmens, Dmitry Dedov, Jon Fridrik Kjølbro, Mārtiņš Mits, Armen Harutyunyan, Stéphanie Mourou-Vikström, Georges Ravarani, Marko Bošnjak, Tim Eicke, *judges*, and Søren Prebensen, *Deputy Grand Chamber Registrar*.
[1430] *EU Convention, supra* note 1413 at art 8.
[1431] *Bărbulescu Grand Chamber, supra* note 1404 at paras 69–74.
[1432] *Ibid* at paras 74−78.
[1433] *Ibid* at para 80.

discretion enjoyed by Member States could not be unlimited; there needed to be adequate and sufficient safeguards against abuse.[1434]

To that end, the Grand Chamber stated that domestic authorities had to regard the following factors as relevant: (1) whether the employee was notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures; (2) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy; (3) whether the employer provided legitimate reasons to justify monitoring the communications and accessing their actual content; (4) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employees communications; (5) the consequences of the monitoring for the employee subjected to it; and (6) whether the employee was provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature.[1435] Also, the Grand Chamber highlighted that it was critical that the employee whose communications had been monitored had access to a remedy before a judicial body with jurisdiction.[1436]

When applying these principles, the Grand Chamber concluded that, by virtue of the positive obligations under Article 8 of the *EU Convention*,[1437] the national authorities were required to carry out a balancing exercise between competing interests, namely Bărbulescu's right to respect for private life and correspondence with E's business interests.[1438] In this case, the domestic courts failed to determine: whether Bărbulescu had received prior notice of the possibility that his communications on Yahoo! Messenger might be monitored; whether he had been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence; the specific reasons justifying the introduction of the monitoring measures; whether E could have used measures entailing less intrusion into Bărbulescu's private life and

---

[1434] *Ibid* at para 120.
[1435] *Ibid* at para 121.
[1436] *Ibid* at para 122.
[1437] *EU Convention*, *supra* note 1413 at art 8.
[1438] *Bărbulescu Grand Chamber*, *supra* note 1404 at paras 124, 127.

correspondence; and whether the communications might have been accessed without his knowledge.[1439]

Consequently, notwithstanding Romania's margin of appreciation, the Grand Chamber (by 11 votes to six) concluded that there was a violation of Article 8 of the *EU Convention*[1440] since the domestic courts did not afford adequate protection of Bărbulescu's right to respect for his private life and correspondence, and they consequently failed to strike a fair balance between the interests at stake.[1441] Bărbulescu was awarded a monetary amount for costs and expenses.[1442]

5.5.2 Analysis of *Bărbulescu*

This case involved the following features of workplace privacy cases: Bărbulescu was successful in his claim; the matter took place in a court;[1443] the surveillance scenario involved the discovery of employee misuse of technology; the electronic surveillance technology involved the monitoring of electronic communications, namely Yahoo! Messenger activity; and the misconduct took place while Bărbulescu was on-duty.

My goal in this section is to extract principles and values from *Bărbulescu*. First, I will set out the challenges associated with balancing the competing interests and also the principles that emerge from this workplace privacy case. Second, I will stress the importance of being informed about the monitoring and related details. And third, I will consider the unique aspects of the employment relationship and the need for some flexibility, while still ensuring that there are adequate safeguards are in place.

[1439] *Ibid* at paras 124–140.
[1440] *EU Convention, supra* note 1413 at art 8.
[1441] *Bărbulescu Grand Chamber, supra* note 1404 at paras 140–141.
[1442] *Ibid* at para 152. Though the finding itself was found to be sufficient just satisfaction for the non-pecuniary damage suffered, the monetary award for costs and expenses was €1,365.
[1443] The decisions regarding this case that I will be examining in detail are court decisions, namely the Fourth Section and Grand Chamber. Since this case has spanned over 10 years, there are several levels of decisions in forums that the Fourth Section and Grand Chamber collectively refer to as "domestic courts". Also, as mentioned above, my discussion of legislation is limited to the European Union instruments. See *supra* note 1409.

To this end, the first thing to note about this case was that the Grand Chamber confirmed that it was necessary to conduct a careful balance of the competing interests; in this case, the domestic courts did not afford adequate protection of Bărbulescu's right to respect for his private life and correspondence, since they failed to strike a fair balance between the interests at stake.[1444] More precisely, the Grand Chamber concluded that the domestic courts failed to determine: whether Bărbulescu had received prior notice of the possibility that his communications on Yahoo! Messenger might be monitored; whether he had been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence; the specific reasons justifying the introduction of the monitoring measures; whether E could have used measures with less of an intrusion into Bărbulescu's private life and correspondence; and whether the communications might have been accessed without his knowledge.[1445]

The case highlighted the difficulties in balancing the interests of parties in employment relationships, where a prime feature is the unequal bargaining power.[1446] Bărbulescu was repetitively unsuccessful since his termination in August 2007, and it was not until the decision of the Grand Chamber that he was successful with his claim in September 2017 (10 years later).[1447] However, the decision of the Grand Chamber was not unanimous, given that there was a split of 11 to six.[1448] In light of the significant dissent in the Grand Chamber, the case showed the challenges that arise when attempting to simultaneously protect both the right to respect for private life and correspondence of employees and the legitimate business interests of employers.[1449]

On one hand, there were several arguments justifying why E would want to conduct electronic surveillance of employees' communications to meet its legitimate business interests, and why the domestic courts would put considerable weight on these interests

---

[1444] *Bărbulescu Grand Chamber, supra* note 1404 at para152.
[1445] *Ibid* at paras 124–140.
[1446] *Machtinger, supra* note 1131 at para 31; *Wallace, supra* note at 1132 paras 92−93. See also David Doorey, "Common Law and Regulation", *supra* note 1131 at 5−6, 67−75, 111−120; David Doorey, "Industrial Relations and Collective Bargaining", *supra* note 1131 at 67, 94−97, 239−241.
[1447] *Bărbulescu Grand Chamber, supra* note 1404 at paras 11−152.
[1448] *Ibid* at 46−56.
[1449] *Ibid.*

during the balancing. For instance, the County Court noted several reasons why E would want to monitor Bărbulescu and his coworkers, including preventing damage of company IT systems, preventing the commission of illicit activities in the company's name, and preventing employees from revealing company secrets.[1450] The Court of Appeal opined that it was necessary and reasonable to monitor communications because it was the only way to establish that there was a disciplinary breach.[1451] In fact, the Court of Appeal went so far as to say that employers had the right and the obligation to ensure the functioning of their companies, and this included checking the manner in which employees completed their professional tasks.[1452] Moreover, the Fourth Section was of the view that it was understandable that E accessed the Yahoo! Messenger account because there was an assumption that the information in question had been related to professional activities (since this was what Bărbulescu told E, and of course, that was the rule).[1453] The Fourth Section stated that it was not unreasonable for an employer to want to verify that employees were completing their professional tasks during work hours.[1454] Further, the dissenting judges at the Grand Chamber asserted that, while the domestic courts may have attached a greater weight to the employer's right to ensure the smooth running of the company, those courts enjoyed discretion when striking the balance between the parties' interests.[1455] In this case, the dissenting judges were of the view that employers were entitled to check that their employees were carrying out their professional duties when making use of company equipment in the workplace and during working hours.[1456] They also pointed out that the monitoring in this case was limited in time and scope, and the domestic courts took into account Bărbulescu's denial that he ever used company resources for personal purposes.[1457] The dissenting judges emphasized that Bărbulescu never denied that he was informed about the monitoring, and he just could not remember

---

[1450] *Bărbulescu Fourth Section, supra* note 1401 at para 10.
[1451] *Ibid* at para 12.
[1452] *Ibid.*
[1453] *Ibid* at paras 54, 57, 63.
[1454] *Ibid* at paras 58–60.
[1455] *Bărbulescu Grand Chamber, supra* note 1404 at 54. The dissenting judges were Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström, and Eicke.
[1456] *Bărbulescu Grand Chamber, supra* note 1404 at 54.
[1457] *Ibid* at 55.

when he was informed.[1458] Another relevant point was that the dissenting judges did not look favourably on the broken bond of trust in the employment relationship because of Bărbulescu's attitude and denial of ever using the work account for personal reasons.[1459] They appeared to pick up on E's feelings of betrayal, which had the potential of destroying the employment relationship.[1460]

On the other hand, there were some noteworthy reasons why Bărbulescu would want to argue that he was entitled to protection of the right to respect for his private life and correspondence and why the domestic courts would give substantial weight on these interests during the balancing. This can be seen when examining Bărbulescu's arguments. First, Bărbulescu argued that his communications were private since they were with his fiancée and brother, and also involved sensitive health issues.[1461] Second, E accessed both his professional and his personal Yahoo! Messenger accounts, even though they had a different ID numbers, and this went beyond what was necessary.[1462] Third, E generated a 45-page transcript, and somehow allowed all of his coworkers to see this transcript such that his sensitive health information was circulated and discussed among his coworkers.[1463] Fourth, if he had known that his communications were not private, he never would have disclosed his intimate information or created a password.[1464] Fifth, he truly did not know about the extent of the monitoring, and neither the Internal Regulations nor the notice to employees constituted proper notice of the monitoring.[1465]

And the Grand Chamber agreed with Bărbulescu that there was a violation of Article 8 of the *EU Convention*,[1466] since there was a failure to strike the proper balance between the competing interests of the parties.[1467] There was some question about whether there really was a valid notice to employees warning of the nature, extent, and consequences of the

---

[1458] *Ibid.*
[1459] *Ibid.*
[1460] Hicks, *supra* note 1129 at 95−96.
[1461] *Bărbulescu Fourth Section, supra* note 1401 at paras 29–30.
[1462] *Ibid* at para 31.
[1463] *Ibid* at paras 7, 31.
[1464] *Ibid* at 33.
[1465] *Ibid.*
[1466] *EU Convention*, *supra* note 1413 at art 8.
[1467] *Bărbulescu Grand Chamber, supra* note 1404 at paras 124–141.

monitoring, and this caused decision makers to disagree; there were also some timing issues concerning when the notice was read and signed by Bărbulescu after it was circulated.[1468]

Regardless of whether one agrees with the results of the balancing exercise performed by the Grand Chamber, it is important to note that several critical principles and values emerge from the discussion. For instance, the Grand Chamber referred to several important data protection principles stemming from the *Data Protection Directive* that was in effect at the time and that applied to the monitoring of Internet and email use in the workplace.[1469] In particular, the principle of necessity requires monitoring to be necessary to achieve a certain aim.[1470] The principle of purpose specification requires data to be collected for specified, explicit and legitimate purposes.[1471] The principle of transparency requires employers to provide employees with full information about monitoring operations.[1472] The principle of legitimacy requires data-processing operations to only take place for a legitimate purpose.[1473] The principle of proportionality requires that the personal data being monitored had to be relevant and adequate in relation to the specified purpose.[1474] The principle of security requires employers to take all possible security measures to ensure that the data collected are not accessible to third parties.[1475] The Grand Chamber also clarified proportionality, citing the Article 29 Working Party in its Opinion 8/2001,[1476] and stated that any monitoring of employees had

---

[1468] *Ibid* at paras 14–17. According to the Grand Chamber decision, Bărbulescu signed the notice sometime between July 3, 2007 and July 13, 2007. E monitored communications in real time from July 5, 2007 to July 13, 2007. Bărbulescu had been aware of the Internal Regulations since December 20, 2006.
[1469] *Bărbulescu Grand Chamber, supra* note 1404 at para 30.
[1470] *Ibid.*
[1471] *Ibid.*
[1472] *Ibid.*
[1473] *Ibid.*
[1474] *Ibid.*
[1475] *Ibid.*
[1476] Article 29 Data Protection Working Party, "Opinion 8/2001 on the Processing of Personal Data in the Employment Context, WP 48" (13 September 2001) at 3−4, online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf> [Working Party, "Opinion 8/2001"].

to be proportionate to the risks employers faced, taking into account the legitimate privacy and other interests of workers.[1477]

Additionally, the Grand Chamber listed several factors that were relevant when conducting the balancing of competing interests, which I will call the "Bărbulescu Principles": (1) whether the employee was notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures; (2) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy; (3) whether the employer provided legitimate reasons to justify monitoring the communications and accessing their actual content; (4) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employees communications; (5) the consequences of the monitoring for the employee subjected to it; and (6) whether the employee was provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature.[1478] Lastly, though not a numbered item, it is also required that the domestic authorities should ensure that an employee has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful.[1479]

In my view, the essence of the above-mentioned principles could be harmonized into a new Canadian workplace privacy regime. One may disagree and point out that these principles were developed in a different cultural context and use what could be viewed as a different theoretical approach to privacy, namely the dignity/human rights approach.[1480]

[1477] *Bărbulescu Grand Chamber, supra* note 1404 at para 46.
[1478] *Ibid* at para 121.
[1479] *Ibid* at para 122.
[1480] As discussed in Chapter 4, only Québec has enacted a right to privacy. Canada data protection legislation currently asks the question of what a reasonable person would consider to be appropriate in the circumstances. The approach is in line with the pragmatic approach to privacy focused on the appropriate flow of information and reasonable expectations, and also deals with consent, in line with the control-over-information through limited access approach to privacy. See *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 3 ("a reasonable person would consider appropriate in the circumstances") and Schedule 1, cl 4.3 (dealing with the core concept of consent); *R v Spencer*, 2014 SCC 43 at paras 34−47; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social*

In fact, one may wish to remind me of the importance of respecting cultural contexts of laws examined in other jurisdictions and refraining from hastily performing legal transplants.[1481] However, I would like to suggest that, if we are operating under the assumption that data protection legislation will soon be revamped to become more rights-based as I also proposed in Chapter 4,[1482] then it would not be too far-reaching to carefully borrow some of these novel ideas that stem from the European Union workplace privacy cases, and strategically incorporate them into Canada's workplace privacy regime.

To recap, I have just explained the challenges associated with balancing the competing interests and also the Bărbulescu Principles. The second thing that I will do is highlight the importance of being informed about the monitoring.

To that end, it is critical to ensure that employees are properly informed of any workplace rules and also the nature, extent, and consequences of monitoring communications.[1483] Most importantly, as explained by the Grand Chamber, the notice had to come *before* the monitoring was commenced by the employer.[1484] Not only did the nature and extent of the monitoring activity have to be made clear to the employees, but the possibility of accessing the contents of the communications had to be spelt out as well.[1485]

In this case, the Grand Chamber confirmed that there may have been notice of the ban on personal Internet use, but it was not so clear that Bărbulescu had been informed

---

Life (Stanford: Stanford University Press, 2010) at 1−2, 231–233; Ruth Gavison, "Privacy and the Limits of the Law" in David Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 346 at 348; Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (New Jersey: Rowman & Littlefield, 1988) at 3; Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1968) at 7; W A Parent, "A New Definition of Privacy for the Law" (1983) 2 Law and Philosophy 305 at 306; Raymond Wacks, *Personal Information: Privacy in the Law* (Oxford: Clarendon Press, 1989) at 15–16.

[1481] Samuel, *supra* note 1095 at 124–134; Van Hoecke, *supra* note 1094 at 3−6, 11, 28, 30; Siems, *supra* note 1095 at 136−138.

[1482] See Chapter 4, Theme 1.

[1483] *Bărbulescu Grand Chamber, supra* note 1404 at paras 74–78.

[1484] *Ibid*.

[1485] *Ibid.*

beforehand that monitoring of his communications was going to take place, about the nature and extent of the monitoring activity, or of the possibility that E could access the contents.[1486]

Additionally, the Grand Chamber clearly stated that employers were allowed to create workplace rules and put in place some restrictions that affected employees' respect for private life and privacy of correspondence, but these restrictions could not be imposed entirely, to the point where the right to private social life in the workplace was reduced to zero—the right to private life and privacy of correspondence continued to exist, even if it was subject to restrictions.[1487]

Judge Pinto de Albuquerque, the dissenting judge in the Fourth Section,[1488] who would have found a violation of Article 8 of the *EU Convention*[1489] in line with the Grand Chamber, provided some important clarifications regarding surveillance policies and notifications about monitoring in the workplace. More explicitly, he stated that it had to be clear to employees that there was an Internet usage policy, and only targeted surveillance regarding well-founded suspicions of policy violations were acceptable.[1490] He specifically elaborated on the reason for this principle: without a fair policy in place, Internet surveillance in the workplace could be abused by employers, "acting as a distrustful Big Brother lurking over the shoulders of their employees, as though the latter had sold not only their labour, but also their personal lives to employers".[1491] Essentially, he insisted that it was necessary to avoid such commodification of workers and make responsible policies on Internet use.[1492] With respect to the notice of monitoring, Judge de Albuquerque stated that proper notice of monitoring was critical; not only did it have to be provided, but it also had to be properly drafted so that it was clear enough to understand.[1493] And rules and consequences had to be proportionate.[1494]

[1486] *Ibid*.
[1487] *Ibid* at para 80.
[1488] *Bărbulescu Fourth Section, supra* note 1401.
[1489] *EU Convention, supra* note 1413 at art 8.
[1490] *Bărbulescu Fourth Section, supra* note 1401 at 23.
[1491] *Ibid* at 25.
[1492] *Ibid*.
[1493] *Ibid* at 27–29.

Indeed, electronic surveillance that goes beyond what is necessary is detrimental to employees; it is important for management to avoid the temptation to extend the monitoring beyond what is required.[1495] For instance, some of the dangers of excessive monitoring in the workplace include reduced motivation levels, increased negative physical symptoms such as pain, increased psychological symptoms such as anxiety and depression, reduced trust levels, and increased levels of behaviours that the surveillance was designed to prevent such as sabotage, refusal to meet expectations, and manipulation of the boundaries.[1496]

Therefore, it is important to take heed of Judge de Albuquerque's warning, acknowledge the dignity of workers, and treat them as ends in themselves rather than just as means to achieve a particular goal.[1497]

I have therefore explained how important it is to inform and provide details about the monitoring, something that is unique to the European Union's novel approach. The third thing that I will do is discuss the unique aspects of the employment relationship and the need for some flexibility, while still ensuring that adequate safeguards are in place.

More precisely, the Grand Chamber recognized the uniqueness of the employment relationship, and how there were special features that had to be addressed.[1498] The Grand Chamber emphasized that, from a regulatory point of view, the law left room for negotiation between the parties in respect of their employment contracts.[1499] Moreover, the Grand Chamber stated that, although a small number of Member States explicitly regulated respect for private life and correspondence in the workplace because of the

---

[1494] *Ibid*.
[1495] Kirstie Ball, "An Overview", *supra* note 1343 at 93–94.
[1496] *Ibid*; Kirstie S Ball & Stephen T Margulis, "Electronic Monitoring and Surveillance in Call Centers: A Framework for Investigation" (2011) 26:2 New Technology, Work and Employment 113 at 116–117, online (pdf): *Wiley Online Library* <https://onlinelibrary.wiley.com/journal/1468005X> [Ball & Margulis, "Framework"].
[1497] *Bărbulescu Fourth Section, supra* note 1401 at 25; Hunt, *supra* note 1308 at 203.
[1498] *Bărbulescu Grand Chamber*, *supra* note 1404 at paras 118–119.
[1499] *Ibid.*

margin of appreciation they enjoyed, it was important to keep in mind that their discretion could not be unlimited.[1500] That is, it was still necessary for domestic authorities to ensure that employers used adequate and sufficient safeguards against abuse.[1501]

There is a range of technologies that can be used in the workplace, from computer logging, telephone logging, CCTV monitoring, to mobility tracking.[1502] The Internet has played a large role in the increase of employee monitoring, and it is fairly common for companies to monitor worker communications and activities on the work premises.[1503] In fact, the Internet has allowed for electronic measurements of performance such as keystrokes or telephone call content, or communications such as email and web monitoring; likewise, it has allowed for the electronic tracking of behaviours including location devices such as pagers, CCTV, GPS, and RFID, or covert surveillance (for instance, hidden cameras).[1504] Employers can also conduct electronic monitoring of personal characteristics such as biometrics (bodily measurements such as electronic fingerprinting or retina and iris scanning), data mining, headhunting, and e-recruitment.[1505] Electronic workplace surveillance and business organizations go hand-in-hand; electronic surveillance in the workplace simply replaces older forms of surveillance such as clocking-in or counting and weighing output for payment by piece-rate.[1506] Viewed as a good management practice, it is often considered necessary and a normal element of working life that has been taken for granted, so much so, that employees often expect to have their performance reviewed and their information gathered on their professional activities and whereabouts.[1507]

However, there is a potential for abuse of surveillance power in the workplace, and this is why it is necessary to have protections in place—especially when the monitoring goes

---

[1500] *Ibid* at para 120.
[1501] *Ibid.*
[1502] Kirstie Ball, "An Overview", *supra* note 1343 at 88.
[1503] *Ibid.*
[1504] *Ibid* at 90–91.
[1505] *Ibid.*
[1506] *Ibid* at 89.
[1507] *Ibid.*

beyond what is considered reasonable or when employers demand exacting and precise information as to how employees use their time.[1508] The privacy concerns associated with covert surveillance of electronic communications are significant, especially given the technological capacity to record and store these communications, some of which could contain sensitive confidential information as in this case.[1509] Also concerning for employees is the fact that some of these communications could be stored on offshore servers in different jurisdictions that are subject to different rules governing privacy.[1510]

It is clearly necessary to respect employees' inherent value and worth.[1511] As exhibited in the decision of the Grand Chamber, privacy is an essential human need, and employers are not permitted to completely prevent employees from enjoying this facet of human life.[1512] Privacy cannot be reduced to zero.[1513]

In this part, I extracted principles and values from *Bărbulescu*. I fulfilled this by noting the challenges associated with balancing the competing interests and the Bărbulescu Principles that emerged from this workplace privacy case, the importance of being informed about the monitoring and details of the monitoring, as well as the unique aspects of the employment relationship and the need to allow for some flexibility, while still ensuring that adequate safeguards are in place.

5.5.3 Implications for the New Workplace Privacy Regime

The preceding analysis points to the challenges faced when attempting to balance interests of the parties in privacy cases. It also highlights essential principles that are used in order to accomplish this balancing analysis. I contend that there needs to be provisions that incorporate the Bărbulescu Principles, where employers are required to create policies and procedures regarding electronic surveillance of communications inside the

---

[1508] *Ibid.*
[1509] *Ibid* at 92.
[1510] *Ibid.*
[1511] Hicks, *supra* note 1129 at 2.
[1512] Alexandra Rengel, *Privacy in the 21st Century* (Netherlands: Koninklijke Brill, 2013) at 1; *Bărbulescu Grand Chamber, supra* note 1404 at para 80.
[1513] *Bărbulescu Grand Chamber, supra* note 1404 at para 80.

workplace. To prevent against the abuse of surveillance power, the policies and procedures would inform employees of the nature of electronic surveillance, extent (including the four temporal dimensions) of the electronic surveillance, degree of intrusion and exactly what the employer wishes to access (solely time codes, content, specific metadata involving the communications), and the disciplinary consequences that can result from the electronic surveillance of the communications. It is also necessary, when dealing with sensitive personal data, to have a provision requiring employers to conduct electronic surveillance of employees' communications in the most ethical manner possible to enhance trust in the employment relationship. There also needs to be provisions enabling the employers and employees to have the flexibility required to jointly create further rules regarding electronic surveillance applying in their specific workplace (in the rare circumstances where employees can freely consent).

5.6 *López Ribalda*

The second European Union workplace privacy case that is discussed in this dissertation is *López Ribalda*. I first describe the facts, history, and decision of the workplace privacy case; I then analyze the case and discuss the implications for the new workplace privacy regime.

5.6.1 The Facts, History, and Decision

Five Spanish employees, who I will call "A", "B", "C", "D", and "E", worked as cashiers for MSA, a family-owned supermarket chain.[1514] MSA noticed that there were some irregularities between supermarket stock levels and what was actually sold; in fact, the supervisor found monthly losses of over €7,780, €17,971, €13,936, €18,009, and €24,614 over five consecutive months.[1515] MSA decided to investigate by installing surveillance cameras, some of which were visible and some were hidden; the visible cameras were pointed toward the entrances and exits of the supermarket to detect any customer thefts, and the hidden cameras were zoomed in on the checkout counters and covered the area

[1514] *López Ribalda and Others v Spain*, Application 1874/13 and 8567/13, Judgment of the Court (Third Section), 9 January 2018 at para 6 [*López Ribalda Third Section*].
[1515] *Ibid* at para 7.

behind the cash desk to detect any employee thefts.[1516] MSA only gave the employees prior notice of the installation of visible cameras.[1517]

Eventually, A, B, C, D, and E were caught, and they each admitted to the thefts in the presence of both their union representative and MSA's legal representative.[1518] More precisely, they were dismissed because they were caught on video helping coworkers and customers steal items and stealing items themselves; they accomplished this by scanning items from the grocery baskets of customers and coworkers and canceling the purchases, and then allowing the customers and coworkers to walk out of the store without paying for the items.[1519] While C, D, and E signed settlement agreements agreeing to not bring any wrongful dismissal proceedings against MSA in exchange for MSA not bringing criminal charges against them for theft, ultimately, A, B, C, D, and E all ended up launching unfair dismissal proceedings at the Granollers Employment Tribunal no 1 (Employment Tribunal), and were unsuccessful.[1520] They appealed to the High Court of Justice of Catalonia (High Court), and were also unsuccessful.[1521] Further appeals, including to the Constitutional Court, were all dismissed.[1522]

In response, A, B, C, D, and E made applications to the European Court of Human Rights, Third Section (Third Section) against the Kingdom of Spain (Spain).[1523] They argued that the covert video surveillance seriously interfered with their right to privacy, and MSA ordered covert video surveillance without previously informing them, thus their rights to private life protected by domestic data protection laws and the Article 8 of the *EU Convention*[1524] were violated.[1525] On the other hand, Spain argued that MSA was a

---

[1516] *Ibid* at para 8.
[1517] *Ibid.*
[1518] *Ibid* at para 9.
[1519] *Ibid* at paras 11, 18.
[1520] *Ibid* at paras 12, 14−15, 19−21. An analysis of the domestic laws of European Union Member States is outside the scope of this dissertation. This discussion is confined to the European Union instruments.
[1521] *Ibid* at para 16, 22.
[1522] *Ibid* at para 17, 23.
[1523] *Ibid* at para 1. The Chamber was composed of: Helena Jäderblom, President, Luis López Guerra, Dmitry Dedov, Pere Pastor Vilanova, Alena Poláčková, Georgios A. Serghides, Jolien Schukking, judges, and Stephen Phillips, *Section Registrar.*
[1524] *EU Convention, supra* note 1413 at art 8.
[1525] *López Ribalda Third Section, supra* note 1514 at paras 3, 43–44.

private company, and any violations (including lack of notice of monitoring) could not be attributed to Spain.[1526] Also, the employees were informed of the installation of the overt video surveillance for theft prevention purposes, but not regarding the covert video surveillance near the cash desks; every citizen had the right to complain about covert video surveillance pursuant to domestic data protection laws to the Data Protection Agency, where MSA could be administratively sanctioned.[1527]

The Third Section stated that private life was interpreted broadly and extended to aspects relating to personal identity, including name and picture.[1528] Also, covert video surveillance of employees was viewed as a considerable intrusion into private life, since it involved recording and reproducing documentation about an employee's conduct at work, which was a place where the employee had to be and could not evade.[1529] The Third Section found that Spain did not strike a fair balance between the employees' right to respect for their private life and MSA's interests in protecting its property.[1530] The domestic courts acknowledged that MSA did not comply with the obligation to inform the employees about the installation of the covert video surveillance or of their rights under the data protection legislation.[1531] The surveillance did not involve suspicion aimed at particular employees; rather, there was a general suspicion against all staff, so the surveillance was aimed at all employees working on the cash registers.[1532] Thus, the Third Section decided that there was insufficient proportionality of MSA's measures with the legitimate aim of protecting interests in the protection of property rights.[1533] The video surveillance was aimed at all staff on the cash registers, "over weeks, without any time-limit and during all working hours";[1534] MSA conducted the covert surveillance over a prolonged period of time, and did not comply with requirements to inform the employees of the existence of the system of video surveillance or provide them with the

---

[1526] *Ibid* at paras 47, 50.
[1527] *Ibid* at paras 48−49.
[1528] *Ibid* at paras 54–56.
[1529] *Ibid* at para 59.
[1530] *Ibid* at paras 61, 70.
[1531] *Ibid* at para 65.
[1532] *Ibid* at para 68.
[1533] *Ibid* at para 69.
[1534] *Ibid* at para 68.

necessary information about their rights under data protection laws.[1535] Thus, there was a violation of Article 8 of the *EU Convention*[1536] (by six votes to one), and the employees were awarded monetary amounts for non-pecuniary damage[1537] and costs and expenses[1538] incurred in the proceedings before the domestic courts.[1539]

Spain appealed to the Grand Chamber.[1540] The Grand Chamber stated that there was no question that Article 8 of the *EU Convention*[1541] applied in this case; the employees were subjected to video surveillance at work for a period of 10 days, where the covert cameras were directed towards the supermarket checkout area.[1542] The Grand Chamber emphasized that, though the expectation of privacy was limited in public places, the creation of a systematic or permanent recording of images of identified persons and the subsequent processing of those images could raise questions affecting the private life of the employees.[1543]

The Grand Chamber also clarified the margin of appreciation, and stated that the choice of the means to secure compliance with Article 8 of the *EU Convention*[1544] regarding individuals between themselves fell within the Member State's margin of appreciation,

---

[1535] *Ibid* at paras 68–70.
[1536] *EU Convention, supra* note 1413 at art 8.
[1537] More precisely, they were each awarded €4,000 for moral damages. See *López Ribalda Third Section, supra* note 1514 at para 106.
[1538] More specifically, A received €500, and B, C, D, and E each received €568.86 for costs and expenses. See *López Ribalda Third Section, supra* note 1514 at para 109.
[1539] *López Ribalda Third Section, supra* note 1514 at paras 104−110. Also, the employees claimed that the domestic courts improperly used the surveillance footage to prove the commission of the thefts as the main evidence. See para 46. The Third Section stated that, for Article 6 complaints, the question was not whether evidence that was obtained unlawfully should or should not have been admitted, but whether the proceedings as a whole, including the way in which evidence was taken, were fair. The Third Section dismissed complaints regarding the use of evidence, and also confirmed that there was no reason to challenge the domestic courts' assessment of evidence regarding admissibility of the settlement agreements. A discussion of Article 6 of the *EU Convention* is outside the scope of this dissertation.
[1540] *López Ribalda and Others v Spain*, Applications 1874/13 and 8567/13, Judgment of the Court (Grand Chamber), 17 October 2019 at para 5 [*López Ribalda Grand Chamber*]. The Grand Chamber was composed of: Linos-Alexandre Sicilianos, President, Guido Raimondi, Angelika Nußberger, Robert Spano, Vincent A De Gaetano, Jon Fridrik Kjølbro, Ksenija Turković, Işıl Karakaş, Ganna Yudkivska, André Potocki, Aleš Pejchal, Faris Vehabović, Yonko Grozev, Mārtiņš Mits, Gabriele Kucsko-Stadlmayer, Lətif Hüseynov, María Elósegui, judges, and Søren Prebensen, *Deputy Grand Chamber Registrar*.
[1541] *EU Convention, supra* note 1413 at art 8.
[1542] *López Ribalda Grand Chamber, supra* note 1540 at para 92.
[1543] *Ibid* at para 93.
[1544] *EU Convention, supra* note 1413 at art 8.

and regardless of the discretion enjoyed by Member States when choosing the most appropriate means for protecting rights to respect for private life and correspondence of employees, an employer's monitoring had to be proportionate and have adequate and sufficient safeguards against abuse.[1545] In this case, the Grand Chamber found that Spain had an adequate legal framework with adequate safeguards.[1546]

Also, the Grand Chamber confirmed that the Bărbulescu Principles were transposable to the circumstances of this case on video surveillance in the workplace.[1547] To that end, it examined the Bărbulescu Principles.[1548] It decided that the domestic courts found that there were legitimate reasons for the video surveillance, namely suspicion, given the amount of losses.[1549] Also, the legitimate interests were taken into account by the domestic courts, namely protection of property and smooth functioning of the company.[1550] The degree of intrusion was limited because the covert cameras were only pointed at the checkout area where the losses were likely to occur, so this was reasonable.[1551] Further, the employees worked in a place that was open to the public and involved permanent contact with customers, so there was a lower expectation of privacy (this was in line with the Working Party's Opinion 4/2004[1552]).[1553] The Grand Chamber stated that, though MSA never set a particular duration for the video surveillance beforehand, it was ultimately only for 10 days, and then it ceased as soon as the employees were identified, so this was not excessive.[1554] Also, only the manager, legal representative, and union representative viewed the recordings, so there was not a high

---

[1545] *Ibid* at paras 112–116.
[1546] *Ibid* at para 119.
[1547] *Ibid* at para 116. The Grand Chamber also pointed out that these principles were developed in line with its previous cases, one of which included *Köpke v Germany*, Application 420/07, Judgment of the Court (Fifth Section), 5 October 2010.
[1548] *López Ribalda Grand Chamber, supra* note 1540 at paras 123–136.
[1549] *Ibid* at para 123.
[1550] *Ibid.*
[1551] *Ibid* at para 124.
[1552] Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance, WP 89" (11 February 2004) at 24−25, online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf> [Working Party, "Opinion 4/2004"].
[1553] *López Ribalda Grand Chamber, supra* note 1540 at para 125.
[1554] *Ibid* at para 126.

degree of seriousness of intrusion.[1555] The consequences of the monitoring were serious since the employees involved were dismissed based on the recording, but the domestic courts noted that the recordings were not used for any other purpose except to trace the losses and take disciplinary measures against the employees.[1556] Further, there were no other means to fulfill the legitimate aim, there was a significant possibility that the thefts were committed by more than one person given the losses, and providing any information to the employees could have defeated the purposes of the video surveillance.[1557] Domestic laws adequately prescribed a certain number of safeguards to prevent improper interference with the rights of individuals.[1558]

The Grand Chamber also confirmed that the lack of prior information was justified; in the specific circumstances, given the degree of intrusion and the legitimate interests justifying the video surveillance, the employment courts were able to, without overstepping the margin of appreciation, decide that the interference with the employees' privacy was proportionate.[1559] There was reasonable suspicion of serious misconduct in light of the extent of the losses, and this was especially important in situations where the smooth functioning of the company was endangered by the suspicion of concerted action by several employees (14 employees were dismissed in total)[1560] that created a general atmosphere of mistrust in the workplace.[1561] The Grand Chamber stressed that the employees had other avenues for making complaints, such as complaining to the Data Protection Agency for a failure to fulfill the obligation to provide prior information, and MSA could have received fines.[1562] Thus, it found (by 14 votes to three) that Spain did not fail to fulfill its positive obligations under Article 8 of the *EU Convention*[1563]and there was no violation.[1564]

[1555] *Ibid.*
[1556] *Ibid* at para 127.
[1557] *Ibid* at para 128.
[1558] *Ibid* at para 129.
[1559] *Ibid* at paras 132–134.
[1560] *Ibid* at para 15.
[1561] *Ibid* at para 134.
[1562] *Ibid* at paras 135–136.
[1563] *EU Convention, supra* note 1413 at art 8.
[1564] *López Ribalda Grand Chamber, supra* note 1540 at para 137. Also, the Grand Chamber confirmed findings of the Third Section regarding the use of surveillance images as part of the evidence and validity

5.6.2 Analysis of *López Ribalda*

This case involved the following features of workplace privacy cases: the employees were not successful in their claims; the matter took place in a court;[1565] the surveillance scenario dealt with proactive surveillance operations; the electronic surveillance technology involved both overt and covert video surveillance, namely continuous CCTV monitoring; and the misconduct took place while the employees were on-duty.

This was not the same kind of situation as in *Graphic Packaging*, where T had done nothing wrong while off-duty, but was subject to aggressive covert electronic surveillance that led to his hasty dismissal; there was an abuse of surveillance power when Graphic Packaging rashly commenced the surveillance on T, interpreted the results, and dismissed T. This case was not quite the same as *Bărbulescu* either, since there was no suspicion beforehand that Bărbulescu had done anything wrong; E was monitoring all of the employees' communications in the workplace without any specific reason or target. On the contrary, *López Ribalda* involved a situation where five employees were caught on hidden camera stealing thousands of euros of product from MSA over several months; in light of the amount of losses, MSA appeared to have genuine suspicion when installing the video surveillance cameras to protect its property rights.

My goal in this section is to extract principles and values from *López Ribalda*. First, I will note the challenges associated with balancing the competing interests and principles that emerge from this particular workplace privacy case. Second, I will delve into the

---

of the settlement agreements under Article 6 of the *EU Convention*, deciding (unanimously) that the proceedings, as a whole, had been fair. See paras 149−161. A discussion of Article 6 of the *EU Convention* is outside the scope of this dissertation.

[1565] The decisions regarding this case that I will be examining in detail are court decisions, namely the Third Section and Grand Chamber. However, I acknowledge that this case is a unionized case spanning over 10 years, where initial complaints were heard at the Employment Tribunal; in this case, there are several levels of decisions in forums that the Third Section and Grand Chamber collectively refer to as "domestic courts". As mentioned above, my discussion of legislation is limited to the European Union instruments. See *supra* note 1520.

problematic issues associated with covert and continuous video surveillance. And third, I will argue that the concept of suspicion must be clarified and handled with caution.

To this end, the first thing to observe about this case is the recurring theme of the challenges faced by decision makers who must balance the interests of the parties in difficult cases such as this. The disputatious nature of the case could be seen with the history of the case, where the employees were repetitively unsuccessful since their dismissals in 2009, but were for a moment successful at the Third Section in 2018, and then were ultimately unsuccessful at the Grand Chamber in 2019 (10 years later).[1566] And it is worth noting that there were some noteworthy dissenting opinions at both the Third Section and the Grand Chamber.[1567]

In my view, this case was more contentious than *Bărbulescu,* likely due to the fact that theft was involved, and there may have been a conflation of various ideas concerning violations involving private life and theft, which could have had the effect of intensifying feelings of betrayal of trust. The Grand Chamber picked up on this notion when stating that suspicion of concerted action by several employees created a general atmosphere of mistrust in the workplace.[1568] As discussed throughout the dissertation, trust is essential in the employment relationship; when trust is shattered in employment, the parties experience feelings of violation and betrayal that lead to a complete breakdown in the relationship.[1569] In fact, broken trust in the employment relationship often leads to dismissals being upheld.[1570] Likewise, trust is essential and is at the core of our expectations of privacy as a significant factor in our decisions to share our personal information.[1571] In employment, trust can be damaged when employees are of the view that electronic surveillance systems have been improperly implemented and this can lead

---

[1566] *López Ribalda Grand Chamber, supra* note 1540 at paras 10−40, 137.
[1567] *López Ribalda Third Section, supra* note 1514 at 32–34; *López Ribalda Grand Chamber, supra* note 1540 at 51−55.
[1568] *López Ribalda Grand Chamber, supra* note 1540 at para 134.
[1569] Hicks, *supra* note 1129 at 95−96.
[1570] Bueckert, *supra* note 1130 at 11–12.
[1571] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018) at 50.

to employees simply refusing to comply with management or adopt a more adversarial "us" versus "them" mentality.[1572]

It should come as no surprise, then, that there were conflicting views regarding whether there was a violation of Article 8 of the *EU Convention*[1573] in this case.

On one hand, the findings of the Third Section made sense in many ways. For instance, the court found that private life was interpreted broadly and extended to aspects relating to personal identity, including name and picture.[1574] The Third Section also confirmed that covert video surveillance of an employee was viewed as a considerable intrusion into private life, because it involved recording and reproducing documentation about an employee's conduct at work, which was a place where the employee had to be and could not evade.[1575] The case dealt with using hidden cameras, about which employees were not aware, and this raised serious concerns about private life.[1576] Also, the Third Section noted that the domestic courts already found that MSA did not properly inform the employees about the installation of the covert video surveillance or of their rights under the applicable data protection legislation.[1577] When examining the nature of the surveillance, the Third Section confirmed that the surveillance was not aimed at one particular employee as a result of suspicion, but rather it was directed at all staff because of the general suspicion of employees working near the cash registers.[1578] The Third Section also found that the video surveillance took place over a prolonged period of time, in a continuous manner, during all working hours.[1579] It was understandable then, why the Third Section found that there was inadequate proportionality in this case, and MSA violated Article 8 of the *EU Convention*[1580] when it did not comply with the requirements

---

[1572] Kirstie Ball, "An Overview", *supra* note 1343 at 93–94; Shoshana Zuboff, "Smart Machine", *supra* note 1306 at 344.
[1573] *EU Convention, supra* note 1413 at art 8.
[1574] *López Ribalda Third Section, supra* note 1514 at paras 54–56.
[1575] *Ibid* at para 59.
[1576] *Ibid.*
[1577] *Ibid* at para 65.
[1578] *Ibid* at para 68.
[1579] *Ibid.*
[1580] *EU Convention, supra* note 1413 at art 8.

to inform the employees of the existence of the system of video surveillance and provide them with the necessary information about their rights under data protection laws.[1581]

Yet on the other hand, there were also reasons why the decision did not make sense, as noted by the dissenting judge at the Third Section, Judge Dedov.[1582] For example, the judge opined that there were no other effective means of protecting the MSA's property rights, so it was not possible to interfere with the right to private life to a lesser extent and capture the information that was required.[1583] Also, Judge Dedov believed that there could be no violation since the misconduct (theft) was incompatible with the right to private life under the *EU Convention*[1584] in this case.[1585] Further, based on the amount of losses that were experienced by MSA (between €7,780 and €24,614 per month), it was reasonable to conclude that the losses might have been caused by more than one person, so there was a good chance that the surveillance was indeed necessary.[1586] Judge Dedov did not agree with the result that the employees were allowed to profit from their own wrongdoing.[1587] Judges Poláčková and Vilanova agreed with that point, and thought that the finding of a violation constituted just satisfaction for their non-pecuniary damage.[1588]

Following this decision at the Third Section, I agreed with many of the privacy principles confirmed by the majority regarding the intrusiveness regarding covert and continuous surveillance during all working hours, the need to use the least intrusive methods, and the importance of properly informing employees about video surveillance (overt and covert). However, while the principles coming out of the decision appeared to make sense, there were some aspects of the decision that led to an absurd result. In this sense, I agreed with some of the points made by the dissenting judges. For instance, I believed that the majority decision sent an inappropriate message that it was acceptable for A, B, C, D, and E to complain to the court and rely on human rights and privacy principles to argue that

---

[1581] *López Ribalda Third Section, supra* note 1514 at paras 68–70, 107−110.
[1582] *Ibid* at 32–34.
[1583] *Ibid* at 32.
[1584] *EU Convention, supra* note 1413 at art 8.
[1585] *López Ribalda Third Section, supra* note 1514 at 32.
[1586] *Ibid* at 33.
[1587] *Ibid* at 33–34.
[1588] *Ibid* at 31.

there was a privacy violation; they did so, despite the amount of losses that MSA suffered, and even though they had unclean hands.[1589] This was troubling, given that it was essential to come to the court with clean hands for two main reasons: the first reason was to ensure fairness and protection of the parties (that is, to prevent claimants from engaging in opportunism and benefitting from their own misconduct in the action); the second reason was to maintain the integrity of the court (in particular, to maintain respect for the law, to promote confidence in the administration of justice, and to preserve the judicial process from contamination).[1590] One may go so far as to assert that the employees in this case were acting in line with the economic theoretical approach to privacy, and appeared to be trying to argue for privacy rights to obtain a monetary award that was in addition to the value already realized from the substantial thefts.[1591] In the circumstances, this use of privacy rights to gain further value was concerning.

Upon learning of the upcoming appeal decision, I anticipated that the Grand Chamber would confirm the decision of the Third Section to reinforce the privacy principles on video surveillance, but modify the decision by not awarding monetary amounts to the employees in line with the dissenting opinions of the Third Section. However, the Grand Chamber subsequently released its decision—reversing the Third Section's decision.

In my view, the decision of the Grand Chamber raised a few problematic issues. First, the balancing appeared to be shallow, where the Grand Chamber glossed over one or two of the Bărbulescu Principles per paragraph.[1592] Second, the Grand Chamber also seemed to minimize the fact that MSA never actually had a plan for the duration of the continuous covert video surveillance that was always on for all workers in the area; it just so happened that the employees were caught after 10 days, so the surveillance activity was brought to an end—there was a potential for the electronic surveillance to continue for a

---

[1589] T Leigh Anenson, "Beyond Chafee: A Process-Based Theory of Unclean Hands" (2010) 47:3 Am Bus LJ 509 at 509, 515−519, 528−530 [T Leigh Anenson, "Theory of Unclean Hands"]; T Leigh Anenson, "Announcing the Clean Hands Doctrine" (2018) 51:5 UC Davis L Rev 1827 at 1829, 1837−1847 [T Leigh Anenson, "Clean Hands Doctrine"].
[1590] T Leigh Anenson, "Theory of Unclean Hands", *supra* note 1589 at 509, 515−519, 528−530, 537; T Leigh Anenson, "Clean Hands Doctrine", *supra* note 1589 at 1837−1847.
[1591] Posner, *supra* note 1377 at 394; Rule, *supra* note 1381 at 185.
[1592] *López Ribalda Grand Chamber*, *supra* note 1540 at para 123–136.

longer period of time, without any real safeguards in place.[1593] In my view, this meant that there was a risk of the abuse of electronic surveillance power, and it is unacceptable to downplay this fact. The Grand Chamber barely even touched on the kinds of limits that would need to be used; more was needed than merely stating that it did not appear to be excessive.[1594] Third, I agree with the dissenting judges that it was inappropriate to find that the degree of intrusion was not serious since only the manager, legal representative, and union representative viewed the recordings.[1595] That is, I agree with Judges De Gaetano, Yudkivska, and Grozev that much more attention had to be paid to the power of electronic surveillance technology and the dangers associated with abusing that power, especially when it came to covert video surveillance.[1596] More precisely, electronic surveillance technologies, had the potential to be carried out and transmitted with technological ease, and this became crucial where an employer used covert video surveillance in the workplace.[1597]

Fourth, and most strikingly, I find the decision to minimize the importance of being properly informed somewhat perplexing. More precisely, the Grand Chamber found that, even though the duty to inform had not been met as confirmed by the domestic courts, in this case, the employment courts were able to decide that the interference with the employees' privacy was proportionate.[1598] In my view, this could create some problems. The first problem is that this decision could enable employers to believe that they can engage in numerous instances of covert surveillance without using proper safeguards based on clouded understandings of suspicion. The second problem is that there could be a softening of the requirement to inform over time, where it is transformed into just one of the other factors to consider. The third problem is that allowing the introduction of covert surveillance cameras into the workplace, without properly informing employees or using any real safeguards, could wreak havoc in the workplace and intensify feelings of mistrust between the parties in the employment relationship.

[1593] *Ibid* at para 126.
[1594] *Ibid.*
[1595] *Ibid.*
[1596] *Ibid* at 51.
[1597] *Ibid.*
[1598] *Ibid* at paras 132–134.

The Grand Chamber noted that the legitimate interests were to discover and punish those responsible for the losses, with the aim of ensuring the protection of its property and the smooth functioning of the company.[1599] Also, there was no other way to fulfill the legitimate aim, and an examination of lesser intrusive methods would have defeated the purposes given the extent of the losses.[1600] Yet, in my view, MSA still could have provided proper notification of the covert surveillance cameras in accordance with domestic laws, even in a general manner, and provided A, B, C, D, and E with basic information on their rights as suggested by the Third Section.[1601] In particular, I argue that it was not necessarily true that MSA's approach was the only way to achieve the legitimate purposes. I found it surprising that the Grand Chamber spent so little time deliberating on the process of exploring other lesser intrusive options. I contend that, had A, B, C, D, and E been told of the covert operation, at least they would have better understood their rights in a situation that they could not evade,[1602] and these laws are, after all, considered to be "a certain number of safeguards for the purpose of preventing any improper interference".[1603] The Grand Chamber made such a significant effort in *Bărbulescu* to make the material finding that there was no proper notification in that case;[1604] in contrast, no similar effort was made in this case to acknowledge the import of the factor of proper notification.[1605] Proper notification, after all, is a low threshold to meet, and is not even close to the same thing as consent, as discussed in Chapter 4, Theme 2; it is difficult to see how something this fundamental could be brushed aside. That said, perhaps the Grand Chamber is sending a message that being informed is only one of the Bărbulescu Principles to consider in the balancing analysis to determine proportionality—this could be useful in cases where obtaining consent is not possible (as in employment situations), or properly informing individuals is not practical (as in theft situations where the goal is to discover the identities of thieves and punish them). In this way, considering it as one piece of the proportionality puzzle seems more reasonable.

[1599] *Ibid* at para 123.
[1600] *Ibid* at para 128.
[1601] *López Ribalda Third Section, supra* note 1514 at para 69.
[1602] *López Ribalda Grand Chamber, supra* note 1540 at para 128.
[1603] *Ibid* at para 129.
[1604] *Bărbulescu Grand Chamber, supra* note 1404 at paras 14−17, 74−78.
[1605] *López Ribalda Grand Chamber, supra* note 1540 at paras 132–134.

Regardless of whether one agrees with the Third Section or the Grand Chamber, the Grand Chamber confirmed that the Bărbulescu Principles were transposable to the circumstances of cases involving video surveillance in the workplace.[1606] The Grand Chamber also clarified the meaning of positive obligations and the margin of appreciation for Member States so they can meet their duties to protect private life.[1607] In my view, the explanations and analysis provided in this part of the decision addressed many of the concerns noted by the dissent of the Grand Chamber in *Bărbulescu*.[1608]

Let me pause for a moment and recap. I have just discussed the challenges associated with balancing the competing interests and principles that emerge from this workplace privacy case; I also noted that the Bărbulescu Principles apply to instances of video surveillance. The second thing that I will do is emphasize the serious concerns that arise when dealing with covert and continuous video surveillance.

Thus, it is important to highlight that the Grand Chamber never discounted the Third Section's conclusion that covert, continuous video surveillance of employees was viewed as a considerable intrusion into private life, because it involved recording and reproducing documentation about an employee's conduct at work, which was a place where the employee had to be and could not evade.[1609] In fact, the Grand Chamber noted the significance of creating limits regarding the degree of intrusion, such as putting cameras in limited areas, setting reasonable durations, as well as installing cameras in open, visible, and public areas rather than private areas associated with very high expectations of privacy protection.[1610] Yet in my view, the Grand Chamber failed to

---

[1606] *Ibid* at para 116.
[1607] *Ibid* at paras 110−115.
[1608] *Bărbulescu Grand Chamber, supra* note 1404 at 50–52. The dissenting judges were concerned that the majority did not properly examine Romania's entire framework to determine whether Romania provided sufficient safeguards. The Grand Chamber in *López Ribalda* reviewed Spain's entire framework when confirming that Spain had adequate safeguards in place, and clarified the meaning of a Member State's margin of appreciation regarding private life under Article 8 of the *EU Convention*.
[1609] *López Ribalda Third Section, supra* note 1514 at para 59; *López Ribalda Grand Chamber, supra* note 1540 at para 124.
[1610] *Ibid.*

appreciate the point that employees were being subject to covert continuous video surveillance throughout their entire working day.[1611]

In fact, I argue that this case underscores the critical need to acknowledge, given the nature of electronic surveillance technologies, that there is a serious potential for the abuse of surveillance power when it comes to covert, continuous monitoring—I find it extremely concerning that MSA would consider it appropriate to aim covert cameras "at all the staff working on the cash registers, over weeks, without any time limit and during all working hours".[1612]

One can easily appreciate how covert video surveillance is clearly intrusive, and also dangerous, in light of modern technological capabilities including the recording, storage and dissemination of images.[1613] Indeed, the Office of the Privacy Commissioner of Canada has pointed out the troubling aspects of covert video surveillance, and has stated that there should always be a strong basis for using covert video surveillance, where the information gathered must further that purpose.[1614] Also, there should be proportionality: the loss of privacy needs to be proportional to the benefit gained.[1615] And less privacy-invasive measures should always be tried first.[1616] While there is an acknowledgment that most covert surveillance is conducted without consent, in the employment context, employers should have evidence that the relationship of trust has been broken before conducting covert video surveillance—there must be an evidentiary justification.[1617] The Office of the Privacy Commissioner of Canada has recommended that organizations have a policy on covert video surveillance that sets out privacy-specific criteria that must be met before covert video surveillance is undertaken; requires that the decision be

---

[1611] *López Ribalda Grand Chamber, supra* note 1540 at para 92.
[1612] *López Ribalda Third Section, supra* note 1514 at para 68.
[1613] *López Ribalda Grand Chamber, supra* note 1540 at 51−52; Kirstie Ball, "An Overview", *supra* note 1343 at 92.
[1614] Office of the Privacy Commissioner of Canada, "Guidance on Covert Video Surveillance in the Private Sector" (May 2009), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/> [Privacy Commissioner, "Video Surveillance"].
[1615] *Ibid.*
[1616] *Ibid.*
[1617] *Ibid.*

documented, including rationale and purpose; requires that authorization for undertaking video surveillance be given at an appropriate level of the organization; considers what personal information is necessary to achieve the stated purpose; limits the use of the surveillance to its stated purpose; requires that the surveillance be stored in a secure manner; designates the persons in the organization authorized to view the surveillance; sets out procedures for dealing with third party information; sets out a retention period for the surveillance; and sets out procedures for the secure disposal of images.[1618] It is also important to document specific instances of video surveillance, including how the requirements of the organization's policy on video surveillance have been satisfied: a description of alternative measures undertaken and their result; a description of the kind of information collected through the surveillance; the duration of surveillance; names of individuals who viewed the surveillance; what the surveillance was used for; when and how images were disposed of; and a service agreement with any third party hired to conduct the surveillance, if applicable.[1619]

But it is the Panopticon that provides insights regarding the reasons why continuous monitoring is so troublesome. The Panopticon is associated with the idea of crowded solitude, where there is a chilling vision of individuals packed together yet they are alone.[1620] It is disturbing that the overseer's gaze, daylight, and interiorization can create transparency and a formula where power is exercised continuously for a minimal cost.[1621] The illusion of power is so momentous that individuals become virtuous simply by being observed.[1622] Also unsettling is that this use of disciplinary power creates docile bodies that can be subjected, used, transformed, and improved; in instances of continuous surveillance, visibility becomes a trap that controls individuals.[1623] It remains an alarming fact that continuous monitoring is a type of intensity[1624] that is associated with increased

---

[1618] *Ibid.*
[1619] *Ibid.*
[1620] Janet Semple, *Bentham's Prison: A Study of the Panopticon Penitentiary* (Oxford: Oxford University Press, 1993) at 129, 152, 155.
[1621] Michel Foucault, "Power/Knowledge", *supra* note 1304 at 147, 154–155.
[1622] *Ibid* at 161.
[1623] Michel Foucault, *Discipline & Punish: The Birth of the Prison*, 2nd ed, translated by Alan Sheridan (New York: Vintage Books, 1995) at 135–138, 200 [Michel Foucault, "Discipline & Punish"].
[1624] Clarke & Greenleaf, *supra* note 1220 at 108−109.

power if applied in the subtlest possible way.[1625] Disciplinary power is exercised through the watchers' invisibility, because the watched are not able to see, yet they are subject to compulsory visibility.[1626] In this case, MSA appeared to be using the disquieting strategy of beginning with generalized surveillance and subsequently generating suspects, rather than starting with a suspect to monitor due to suspicion.[1627]

In the Panopticon, those who are watched never know whether they are being watched at any time, so they have to assume that they are always being watched; the idea that anyone could be watching at any time creates high levels of anxiety about being continuously watched by anonymous observers.[1628] This may be why the Panopticon is characterized as both a laboratory of power and a circular cage, because of the potential to take advantage of individuals who are forced to be in that one particular place.[1629] Continuous surveillance, then, creates a large potential for manipulation and exploitation, to the point where the Panopticon has been characterized as an efficient instrument of totalitarian control, ruthless social engineering, and psychological manipulation.[1630]

In workplaces, employers have the ability to take advantage in several ways, since the supervisor performs the same function as an overseer.[1631] With electronic surveillance, information systems create a universal transparency with a startling degree of illumination.[1632] That is, the video screen is the modern version of the central tower.[1633] As a result of continuous and transparent workplace monitoring, workers may feel a loss of autonomy or sense of self-control, feel despair at the prospect of being socially

---

[1625] Michel Foucault, "Discipline & Punish", *supra* note 1623 at 208.
[1626] *Ibid* at 187.
[1627] Mark Andrejevic, "Surveillance in the Big Data Era" in Kenneth D Pimple, ed, *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards* (New York: Springer, 2014) 55 at 58 [Mark Andrejevic, "Big Data Era"].
[1628] Michel Foucault, "Discipline & Punish", *supra* note 1623 at 201−202.
[1629] *Ibid* at 203–204, 208.
[1630] Semple, *supra* note 1620 at 316.
[1631] Kirstie Ball, "An Overview", *supra* note 1343 at 89.
[1632] Shoshana Zuboff, "Smart Machine", *supra* note 1306 at 322.
[1633] *Ibid* at 323.

integrated into the high-technology workplace, and feel loss of unique identity and absence of traditional employment protections.[1634]

I argue that consequent feelings of despair and of being manipulated and controlled may likely be magnified in cases where the video surveillance is both continuous *and* covert in nature; in my view, the compounded effect constitutes an appalling violation. Once made aware, one who was watched might question: who was watching; what were they watching; how often were they watching; when were they watching; what was recorded; who accessed it; was it disseminated or posted online; where was it now; was the image manipulated in any way; how many people know about it now; etcetera. Indeed, this could lead to a situation where the watched become distressed about being continuously watched by anonymous observers after-the-fact. It is understandable then, that once A, B, C, D, and E became aware of the continuous covert video surveillance they experienced in the workplace, they launched a privacy complaint and continued with it for 10 years.

This is why it is necessary to provide adequate protections to employees regarding covert and continuous surveillance, since employees are not able to escape the workplace and would not be in a position to evade such monitoring.[1635] Given the nature of this technology and the potential for abuse of surveillance power, it is necessary to ensure that the dignity of individuals is preserved.[1636]

I have therefore demonstrated that there are serious concerns with regards to covert and continuous video surveillance, especially when they are used simultaneously. The third thing that I will do is argue that the concept of suspicion must be clarified and handled with caution.

Indeed, the Grand Chamber was unclear regarding the concept of suspicion, and this may present some challenges. More precisely, as noted above, no employees were individually

---

[1634] *Ibid* at 404.
[1635] *López Ribalda Third Section, supra* note 1514 at para 59.
[1636] Edward J Bloustein, *Individual & Group Privacy* (London: Transaction Publishers, 2003) at 23.

targeted in this case, yet all employees were captured by the covert cameras.[1637] The Grand Chamber was not particularly instructive with its statement:

> Thus, while [the Court] cannot accept the proposition that, generally speaking, the slightest suspicion of misappropriation or any other wrongdoing on the part of employees might justify the installation of covert video-surveillance by the employer, the existence of reasonable suspicion that serious misconduct has been committed and the extent of the losses identified in the present case may appear to constitute weighty justification. This is all the more so in a situation where the smooth functioning of a company is endangered not merely by the suspected misbehaviour of one single employee, but rather by the suspicion of concerted action by several employees, as this creates a general atmosphere of mistrust in the workplace.[1638]

Simply put, this paragraph could be construed as an invitation for employers to conduct continuous, covert video surveillance of employees whenever there is something more than the slightest suspicion; in cases where there could be more than one employee involved in suspected misconduct, the floodgates open even wider and appear to allow employers additional justification for the use of covert video surveillance. From this statement, it is not clear what "reasonable suspicion", "serious misconduct", "extent of the losses", or "may appear to constitute weighty justification" mean.

Indeed, the dissenting judges of the Grand Chamber were not convinced and stated that, in the absence of a requirement of clear procedural safeguards, the existence of reasonable suspicion of serious misconduct was insufficient in situations involving covert video surveillance and could be used to justify an unacceptably large number of cases.[1639] The dissenting judges also emphasized that the unlimited nature of the video surveillance was significant and should have been given additional weight when assessing proportionality.[1640] They declared that the Grand Chamber was allowing the unlimited use of convert video surveillance in the workplace without affording sufficient legal

---

[1637] *López Ribalda Grand Chamber, supra* note 1540 at para 92.
[1638] *Ibid* at para 134.
[1639] *Ibid* at 54.
[1640] *Ibid.*

safeguards to those whose personal data would be collected and used for purposes unknown to them.[1641]

It is vital to recognize that, when it comes to suspicion, the nature of the electronic surveillance technologies enable the watcher to collect vast amounts of personal data and transform dated strategies of starting with a suspect to monitor due to suspicion, to starting with generalized surveillance and subsequently generating suspects.[1642] There is also a potential to engage in profiling and using the personal data to forecast outcomes in advance in attempt to exert control over the watched.[1643] What is more, video analytics can be especially intrusive given that the goal is to allow computers not just to record, but also to understand, the objects and actions that a camera is capturing; this technology can be used to alert the authorities or others when something or someone who is deemed "suspicious" is detected.[1644] The power of this technology is enormous given the potential to gather mass amounts of personal data; in fact, artificial intelligence that centers on deep learning has propelled the technology to unprecedented levels since computers are allowed to learn on their own when fed large amounts of training data.[1645] For instance, video surveillance capabilities have been enhanced with respect to computer vision.[1646] There are several methods used to watch individuals, such as anomaly detection, which involves using automated surveillance systems to automatically detect and track unusual objects and people.[1647] This involves using detection algorithms to look for abnormal things, or a deviation approach to allow smart cameras to learn what is normal.[1648] There are several dangers associated with video analytics. For example, real-time monitoring with video analytics could lead to situations where a massive amount of data is gathered and analytics are used to sift through the data to find suspicious behaviour.[1649] The

---

[1641] *Ibid* at 54–55.
[1642] Mark Andrejevic, "Big Data Era", *supra* note 1627 at 58.
[1643] *Ibid* at 58−67.
[1644] Jay Stanley, "The Dawn of Robot Surveillance, AI, Video Analytics, and Privacy" (2019) at 3, online (pdf): *American Civil Liberties Union* <https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf>.
[1645] *Ibid* at 5−6.
[1646] *Ibid* at 7.
[1647] *Ibid* at 15.
[1648] *Ibid* at 16.
[1649] *Ibid* at 34.

technology has the alarming potential to constantly monitor and judge physical actions and characteristics.[1650] This can lead to considerable chilling effects with cameras that judge behaviour anonymously, discriminatory consequences due to biased algorithms inaccurately flagging people as suspicious, and an abuse of powerful surveillance infrastructures by their controllers.[1651] This takes suspicion to a new level.

For instance, these systems rely on predictions, and a danger is that the panoptic sort plays a role in forecasting outcomes that are likely for classes of individuals; predictability reduces uncertainty about individual behaviour, and the use of power can induce a desired and predictable reaction.[1652] The goal then, is the pursuit of improvement of predictability.[1653] However, there is a potential for the quality of information to be susceptible to errors of measuring, misinterpretation, and strategic modification such that the analysis becomes flawed and creates even further errors.[1654] The potential for serious exploitation arises because this situation can generate predictions that lead to a loss of trust due to misuse of algorithms when we attempt to clean the data, make it accurate, and turn the development of automated systems over to the machines themselves.[1655] Consequently, this raises significant ethical and privacy issues for organizations in the private sector.[1656] This is why it is necessary to have clear and understandable rules in place when it comes to using suspicion to justify the commencement of video surveillance. In order for there to be trust and a sense of safety in the midst of these technological possibilities, the potential for employers' abuse of surveillance must be reined in, and the dignity of employees must be protected.[1657]

In this part, I extracted principles and values from *López Ribalda*. I reached this goal by discussing the challenges associated with balancing the competing interests and the fact

---

[1650] *Ibid.*
[1651] *Ibid* at 35−36, 39−42.
[1652] Oscar H Gandy, Jr, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, Co: Westview Press, 1993) at 45 [Gandy, Jr, "The Panoptic Sort"].
[1653] *Ibid.*
[1654] *Ibid* at 60−61.
[1655] Mark Andrejevic, "Automating Surveillance", *supra* note 1223 at 7−8, 12.
[1656] Stanley, *supra* note 1644 at 45−46.
[1657] Hicks, *supra* note 1129 at 16–17; Waldman, *supra* note 1571 at 50.

that the Bărbulescu Principles apply in cases of video surveillance, the problematic issues associated with covert and continuous video surveillance, and the need to be clear and be vigilant when dealing with the concept of suspicion.

5.6.3 Implications for the New Workplace Privacy Regime

What the analysis confirms is that, when carrying out the balancing analysis of employee privacy and employer legitimate business interests in situations involving video surveillance, the Bărbulescu Principles apply and can be used to determine whether the electronic surveillance was appropriate and whether there was a fair balance was struck between the parties. It is necessary to have provisions incorporating these principles when addressing issues involving the video surveillance of employees. Moreover, the analysis stresses the importance of acknowledging the troubling aspects of both covert and continuous video surveillance, and their effects on employees. Thus, I argue that there needs to be provisions that provide sufficient protections for employees in order to prevent the abuse of electronic surveillance power by employers. This can be accomplished by having a provision stating that it is not acceptable for employers to conduct continuous covert video surveillance on all employees during all working hours; rather, employers need to first ensure that there is reasonable suspicion (that is clearly defined) regarding certain employees, and use the least intrusive means of obtaining the information, rather than targeting all employees for long periods of time.

5.7 Conclusion

This Chapter has examined a variety of workplace privacy cases and has attempted to extract from them some useful principles and values that will be of help in designing a new workplace privacy regime that can close the electronic surveillance gap in employment.

I examined workplace privacy cases from Canada, the United States, and the European Union that contained several important features that help to provide insights into workplace privacy situations. As mentioned in the Introduction, these features included: (1) employee success in the wrongful termination/privacy claim versus failure in the claim; (2) court versus labour arbitrator; (3) surveillance scenario (proactive surveillance

operations versus discovery of employee misuse of technology); (4) electronic surveillance technology type; and (5) on-duty versus off-duty conduct.

My selections, when taken together, contained a balanced mix of jurisdictions and the features of workplace privacy cases. There was a deliberate attempt to avoid a skewed analysis favouring only one jurisdictional perspective or one kind of situation; in my view, variety enhanced the discussion and allowed for the construction of a stronger workplace privacy regime.

Since the goal of this Chapter 5 was to extract useful elements from the workplace privacy cases in order to create the new workplace privacy regime, I avoided providing descriptions of the state of the law in each jurisdiction. Instead, I chose the most pertinent cases from each jurisdiction for the purposes of extracting components to generate ideas and ultimately create proposed provisions for the new workplace privacy regime. The workplace privacy cases I selected included instructive analyses by decision makers so I could more effectively achieve this goal. In particular, while some cases were more recent than others and came from different locations within the jurisdictions, there were notably interesting aspects about each selected case that ultimately proved useful for the analysis and the production of essential ingredients for making the new workplace privacy regime. This became clear when delving deeper and contrasting the cases for the purposes of isolating additional relevant insights for the purpose of crafting the new workplace privacy regime. Further, both the employment principles and the relevant social theory ideas involving surveillance and privacy played a large role when synthesizing ideas to form the new workplace privacy regime.

This Chapter demonstrated that principles and values could successfully be extracted from the examined workplace privacy cases and could be used to design a new workplace privacy regime to sufficiently close the electronic surveillance gap in a way that could fit into Canada’s legal system.

During my case analyses, the selected workplace privacy cases played a considerable role in facilitating the creation of provisions for the new workplace privacy regime.

For instance, *Steel* shed light on core aspects affecting the employment relationship and data protection, namely trust and balance. It also helped to understand some of the inconsistencies associated with data protection and employment approaches, which led to the creation of more even provisions that focused on the concerns of both employers and employees.

Maxam Bulk Services stressed the importance of having a social media policy, and highlighted the sorts of considerations that must be made when crafting such a policy. It also uncovered important employment principles, such as progressive discipline, that can be incorporated into the workplace to set standards and manage expectations for employees.

Graphic Packaging was significant for underscoring the dangers of electronic surveillance, namely the abuse of surveillance power. It also emphasized the importance of incorporating important employment principles such as respecting procedures, contracts or collective agreements, and other company policies, when imposing discipline in response to uncovered surveillance information.

Baker Hughes confirmed the crucial legitimate business interest of protecting employees from discrimination and harassment by coworkers, and allowed for an extension of this principle to the online environment. It also provided clarification on the necessary elements of important workplace documents, including policies, procedures, and collective agreements.

Bărbulescu was important for appreciating the nature of electronic surveillance of communications. It also made a significant impact in the analysis involving the balancing of interests to determine whether a fair balance is struck between the parties, since it is now known for generating the Bărbulescu Principles. Moreover, it confirms that the privacy of employees cannot be reduced to zero.

López Ribalda contributed by standing for the proposition that the Bărbulescu Principles are to be used when assessing proportionality in workplace video surveillance cases.

Also, the case was instrumental for understanding the nature and impact of continuous and covert video surveillance in the workplace, and also the concept of suspicion.

I will discuss in Chapter 6 how I propose to fit these principles and values into Canada's legal system.

Chapter 6

6 The New Workplace Privacy Regime

In Chapter 4, I examined privacy provisions from Canada, the United States, and the European Union and organized them according to three themes: (1) foundational principles touching on privacy and electronic surveillance; (2) consent and balancing rights with legitimate interests; and (3) order-making powers, penalties, and fines. These themes were selected because they involve several interesting issues relating to the electronic surveillance gap in employment. As mentioned in the Introduction, these provisions contained three types of features of privacy provisions: (1) constitutional and human rights provisions; (2) data protection provisions; and (3) employment provisions. These features involved different areas of law that were relevant to privacy and contributed to the understanding of privacy and electronic surveillance.

In Chapter 5, I examined six workplace privacy cases from Canada, the United States, and the European Union that contained several features of workplace privacy cases, including: (1) employee success in the wrongful termination/privacy claim versus failure in the claim; (2) court versus labour arbitrator; (3) surveillance scenario (proactive surveillance operations versus discovery of employee misuse of technology); (4) electronic surveillance technology type; and (5) on-duty versus off-duty conduct.

I extracted principles and values to create building blocks when designing the new workplace privacy regime for the purpose of closing the electronic surveillance gap in employment.

It is now time to propose how I will fit my ideas from Chapters 4 and 5 and into Canada's legal system. More specifically, I will discuss some challenges associated with the task of proposing a new workplace privacy regime for Canada; explain the plan with which I have chosen to proceed; review the previous guidance provided by the Office of the Privacy Commissioner of Canada; and provide some examples of legislative provisions that could be used in a new workplace privacy regime.

6.1 Challenges Encountered When Creating the Workplace Privacy Regime

The first challenge that I encountered involved the fact that there are three features of privacy provisions examined in this dissertation, namely constitutional and human rights, data protection, and employment provisions. These represent different areas of law that are relevant to privacy, under which the proposed provisions could be placed.

It is tempting to take each theme and workplace privacy case and propose provisions that fall under each of these areas of law all at once. However, this strategy of simultaneously converting all ideas into proposed provisions falling under all of these areas of law would not be realistic, since this task would be too complicated, impractical, and time-consuming to implement. Hence, it is necessary to be selective and focus on one or two.

To that end, I will focus on the examination of data protection and employment for the purposes of creating proposed provisions for the workplace privacy regime and fitting them into Canada's legal system.

The second challenge that I faced involved Canadian federalism and the consequent jurisdictional issues. Federalism involves the division of powers between two or more orders of government to provide representation for territorial, linguistic, or ethnic differences in the decision-making structures of a State, entrenching differences over time.[1658] One main advantage of federalism is that different communities can experience unity without being strictly unified.[1659] That is, this method of organizing political life recognizes regional and societal diversity and preserves self-government on a local level.[1660] In Canada, there is a balance between the concentration of power at the national level, and the dispersion of power to the provinces; in other words, there is a balance

---

[1658] Douglas Brown, Herman Bakvis & Gerald Baier, *Contested Federalism: Certainty and Ambiguity in the Canadian Federation*, 2nd ed (Oxford: Oxford University Press, 2019) at 1.
[1659] *Ibid* at 2.
[1660] *Ibid* at 3.

between a unitary system (with a high degree of centralization) and a confederal alliance (with a high degree of decentralization).[1661]

A constitution acts as a blueprint for assigning governmental responsibilities and entitlements, and constitutionally defined jurisdiction is one of the main factors for determining relative weights of the resources available to each order of government with respect to their interactions.[1662] A constitution allocates legislative authority so that the scope of such activity is limited to what a constitution permits the legislatures to do.[1663] In particular, legislatures cannot legislate outside their authority since that would be "*ultra vires*", which is Latin for "beyond the powers".[1664] Legislative authority to make laws is a factor in intergovernmental relations; for example, if a government does not have the authority to make certain laws, it would have to work with the government that does have authority in a cooperative manner to try and achieve its goals.[1665]

The *Constitution Act*[1666] is the source of federalism in Canada.[1667] One of the most important features is the division of power in sections 91 and 92.[1668] These sections provide a list of legislative responsibilities for both the federal and provincial levels of government respectively.[1669] Section 91[1670] lists legislative responsibilities for the federal Parliament, some of which include the regulation of trade and commerce and national defence, while section 92[1671] provides a list of responsibilities for the provinces, some of which include property and civil rights and municipalities.

[1661] *Ibid* at 2, 6.
[1662] *Ibid* at 45.
[1663] *Ibid.*
[1664] Angus Stenson, ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010) *sub verbo* "ultra vires".
[1665] Brown, Bakvis & Baier, *supra* note 1658 at 45–46.
[1666] *Constitution Act, 1867* (UK), 30 & 31 Vict, c 3 s 91, reprinted in RSC 1985, Appendix II, No 5 [*Constitution Act*]. This replaced the former *British North America Act* in Canada in 1982.
[1667] Brown, Bakvis & Baier, *supra* note 1658 at 50.
[1668] *Constitution Act, supra* note 1666 at ss 91−92.
[1669] Brown, Bakvis & Baier, *supra* note 1658 at 50.
[1670] *Constitution Act, supra* note 1666 at s 91.
[1671] *Ibid* at s 92.

Jurisdictional issues arise in Canada's federated system regarding the regulation of labour and employment (provincial) and data protection (federal).[1672] Put another way, there are several important jurisdictional elements to note regarding labour and employment and data protection in Canada's private sector. To fully grasp the ramifications of this fact, it is necessary to explore the inner workings of each regime.

Starting with labour and employment, the governance of nonunionized employment is federally, provincially, or territorially regulated, and each jurisdiction has its own version of employment standards legislation.[1673] The content of employment standards legislation of each jurisdiction is similar in nature, and discusses workplace topics including: compensation; employment records; hours of work; overtime; holidays; vacations; leaves of absence; terminations; layoffs; termination pay; severance pay; as well as penalties and offences.[1674]

Likewise, the governance of unionized employment is federally, provincially, or territorially regulated, and each jurisdiction has its own version of labour relations legislation.[1675] The content of legislation of each jurisdiction is comparable and discusses workplace topics including: the establishment of labour relations boards, powers, and

---

[1672] *Ibid* at ss 91(2), 92(13). More specifically, s 91(2) deals with trade and commerce, which includes commercial activities to which privacy legislation applies. Also, s 92(13) deals with property and civil rights with which labour and employment is associated. See also Office of the Privacy Commissioner of Canada, "PIPEDA in Brief" (May 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/> [Privacy Commissioner, "Brief"]; Government of Canada, "The Constitutional Distribution of Legislative Powers" (25 July 2018), online: *Government of Canada* <https://www.canada.ca/en/intergovernmental-affairs/services/federation/distribution-legislative-powers.html>.

[1673] *Canada Labour Code*, RSC, 1985, c L-2 [*Canada Labour Code*]; *Employment Standards Code*, RSA 2000, c E-9; *Employment Standards Act*, RSBC 1996, c 113; *The Employment Standards Code*, CCSM c E110; *Employment Standards Act*, SNB 1982, c E-7.2; *Labour Standards Act*, RSNL 1990, c L-2; *Labour Standards Code*, RSNS 1989, c 246; *Employment Standards Act*, 2000, SO 2000, c 41 [*Employment Standards Act*]; *Employment Standards Act*, RSPEI 1988, c E-6.2; *Act Respecting Labour Standards*, CQLR c N-1.1; *The Saskatchewan Employment Act*, SS 2013, c S-15.1; *Employment Standards Act*, SNWT 2007, c 13; *Labour Standards Act*, RSNWT (Nu) 1988, c L-1; *Employment Standards Act*, RSY 2002, c 72.

[1674] *Ibid*.

[1675] *Canada Labour Code*, *supra* note 1673; *Labour Relations Code*, RSA 2000, c L-1; *Labour Relations Code*, RSBC 1996, c 244; *The Labour Relations Act*, CCSM c L10; *Industrial Relations Act*, RSNB 1973, c I-4; *Labour Relations Act*, RSNL 1990, c L-1; *Trade Union Act*, RSNS 1989, c 475; *Labour Relations Act*, 1995, SO 1995, c 1, Schedule A [*Labour Relations Act*]; *Labour Act*, RSPEI 1988, c L-1; *Labour Code*, CQLR c C-27; *The Saskatchewan Employment Act*, SS 2013, c S-15.1.

remedies; the rights of employees to be members of unions and the rights of employers to be members of employers' organizations; the certification process and voluntary recognition of unions; bargaining rights and revocation of bargaining rights; collective bargaining; collective agreements; mediation; strikes and lockouts; essential services; picketing; arbitration; prohibited practices; along with offences and penalties.[1676]

Therefore, if my goal is to advise Parliament on how to proceed with lawmaking in respect of issues solely related to labour and employment, it is important to mention that Parliament is limited to creating laws only in the federally regulated jurisdiction, namely in the *Canada Labour Code*,[1677] which contains rules regarding the employment standards in Part III, and rules concerning industrial relations in Part I. By federally regulated, I mean that the legislation applies to any work, undertaking or business that is within the legislative authority of Parliament.[1678] In contrast, for example, the Ontario government would be responsible for creating legislative changes to its *Employment Standards Act*[1679] and its *Labour Relations Act*[1680] concerning employment standards and labour relations respectively.

As can be seen from the above discussion, Parliament is limited in that it can only legislate within its jurisdictional authority and thus can only make changes to the federally regulated jurisdiction in labour and employment. This creates a noteworthy

---

[1676] *Ibid.*
[1677] *Canada Labour Code*, *supra* note 1673.
[1678] *Ibid* at s 2. More specifically, section 2 states that these federal works, undertakings, or businesses include: a work, undertaking or business operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada; a railway, canal, telegraph or other work or undertaking connecting any province with any other province, or extending beyond the limits of a province; a line of ships connecting a province with any other province, or extending beyond the limits of a province; a ferry between any province and any other province or between any province and any country other than Canada; aerodromes, aircraft or a line of air transportation; a radio broadcasting station; a bank or an authorized foreign bank within the meaning of section 2 of the *Bank Act*; a work or undertaking that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more of the provinces; a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and a work, undertaking or activity in respect of which federal laws within the meaning of section 2 of the *Oceans Act* apply pursuant to section 20 of that Act and any regulations made pursuant to paragraph 26(1)(k) of that Act.
[1679] *Employment Standards Act*, *supra* note 1673.
[1680] *Labour Relations Act*, *supra* note 1675.

challenge when one strives to make legislative changes involving workplace privacy to apply throughout Canada. Privacy is set up differently in Canada compared to employment, and this adds further complications.

More precisely, in Canada's private sector, the key piece of omnibus privacy legislation is *PIPEDA*.[1681] It applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities, or is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.[1682] Specifically regarding employment, it applies to a federal work, undertaking or business that is within the legislative authority of Parliament.[1683] Though it applies to inter-provincial operations, *PIPEDA* does not apply to organizations operating entirely within provincially regulated jurisdictions where a province has legislation that has been deemed substantially similar to it, and those particular provincial statutes apply instead; Alberta, British Columbia, and Québec all have private sector privacy legislation that has been deemed substantially similar to *PIPEDA*.[1684] More explicitly, *AB PIPA*,[1685] *BC PIPA*,[1686] and *QC Act*[1687] are considered

---

[1681] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
[1682] *Ibid* at s 4(1).
[1683] *Ibid* at s 2(1). More precisely, section 2 states that these federal works, undertakings, or businesses include: a work, undertaking or business operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada; a railway, canal, telegraph or other work or undertaking connecting any province with any other province, or extending beyond the limits of a province; a line of ships connecting a province with any other province, or extending beyond the limits of a province; a ferry between any province and any other province or between any province and any country other than Canada; aerodromes, aircraft or a line of air transportation; a radio broadcasting station; a bank or an authorized foreign bank within the meaning of section 2 of the *Bank Act*; a work or undertaking that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more of the provinces; a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and a work, undertaking or activity in respect of which federal laws within the meaning of section 2 of the *Oceans Act* apply pursuant to section 20 of that Act and any regulations made pursuant to paragraph 26(1)(k) of that Act.
[1684] Canada SOR/2004-219; Canada SOR/2004-220; Canada SOR/2003-374. The following are exemption orders to exempt Alberta, British Columbia, and Québec from the application of Part 1 of *PIPEDA* in respect of the collection, use and disclosure of personal information in those provinces as they have been deemed substantially similar to *PIPEDA*. A discussion of the personal health information statutes in Canada is outside the scope of this dissertation.
[1685] *Personal Information Protection Act*, SA 2003, c P-6.5 [*AB PIPA*].
[1686] *Personal Information Protection Act*, SBC 2003, c 63 [*BC PIPA*].

to be substantially similar to *PIPEDA*. Further, the two substantially similar provinces, Alberta and British Columbia, have privacy laws that apply to employment information.[1688]

Declaring provincial legislation substantially similar allows the provinces and territories the flexibility to adapt and tailor their own private sector legislation to the specific needs and conditions of their jurisdiction while meeting the intent of *PIPEDA*.[1689] Since *PIPEDA* is considered to be the threshold or floor, substantially similar legislation must be equal to or superior to *PIPEDA* in the degree and quality of privacy protection.[1690] Substantially similar provinces are expected to: incorporate the ten principles in Schedule 1 of *PIPEDA*[1691] (they do not have to be enumerated distinctly, but they must all be present); provide for independent and effective oversight and redress mechanism with powers to investigate; and restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.[1692]

Indeed, there are several complexities when it comes to the application of privacy legislation in Canada, especially in light of the interplay between *PIPEDA*, *AB PIPA*, and *BC PIPA*. Perhaps the Office of the Privacy Commissioner of Canada has most effectively summarized the situation regarding application:

[1687] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 [*QC Act*].
[1688] *AB PIPA, supra* note 1685 at s 4; *BC PIPA, supra* note 1686 at s 3.
[1689] Notice (Industry Canada), (2002) C Gaz I 2388 (Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council) [*Notice*].
[1690] *Ibid* at 2387.
[1691] *PIPEDA, supra* note 1681 at Schedule 1.
[1692] *Notice, supra* note 1689 at 2388. See also Office of the Privacy Commissioner of Canada, "Provincial Legislation Deemed Substantially Similar to PIPEDA" (29 May 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/>.

What are key points about *PIPEDA*, *PIPA* Alberta and *PIPA* BC?

- *PIPEDA* applies to federal works, undertakings or businesses (FWUBs).
- *PIPEDA* applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders. *PIPEDA* also applies within provinces without substantially similar private sector privacy legislation.
- *PIPEDA* applies to employee information only in connection with a FWUB.
- The provincial *PIPA*s apply to provincially regulated private sector organizations.
- Employee information held by provincially-regulated organizations in Alberta and B.C. is covered by the provincial *PIPA*s[1693]

To that end, the Office of the Privacy Commissioner of Canada suggests that organizations ask themselves a few questions in order to determine what private sector privacy law applies to them.[1694] When asking about the province in which the organization operates, if the organization is not a federal work, undertaking or business, and it operates internally in a province with private sector privacy legislation that is deemed to be substantially similar (British Columbia, Alberta, and Québec), then the organization has to comply with that province's law.[1695] If the province does not have private sector privacy legislation, *PIPEDA* is the only statute that would apply.[1696] Also, if considering the issue of employment, *PIPEDA* does not apply to employee information in provincially regulated organizations.[1697] If an organization operates in more than one province, it may have to comply with more than one statute, depending on the jurisdiction.[1698] Regarding the question of interprovincial trade and commerce, such as sending a mailing list from one province to another, trans-border data flows in a commercial context are covered by *PIPEDA* because of the federal government's

---

[1693] Office of the Privacy Commissioner of Canada, "Questions and Answers Regarding the Application of *PIPEDA*, Alberta and British Columbia's *Personal Information Protection Acts*" (November 2004), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/> [Privacy Commissioner, "Questions"].
[1694] *Ibid.*
[1695] *Ibid.*
[1696] *Ibid*.
[1697] *Ibid*.
[1698] *Ibid.*

constitutional power; the same is true for international trans-border data flows, such as sending customer information to a loyalty program in another country.[1699] When asking about the type of organization, organizations are also recommended to look at the definition of "organization" in the particular statute to decide whether it applies.[1700]

Another consideration regarding application is that section 12(1)(a) of *PIPEDA*[1701] states that, before a complainant can make a complaint to the Privacy Commissioner of Canada, the complainant must first exhaust grievance or other review procedures that are otherwise reasonably available; this means that employees in unionized workplaces wishing to make a complaint must first go through the stages of the grievance procedure as discussed in detail in the unionized workplace privacy cases in Chapter 5.[1702]

Therefore, if my goal is to advise Parliament on how to proceed with lawmaking in respect of issues related to privacy in employment, it is important to mention that Parliament is limited to creating laws only in the federally regulated jurisdiction, namely in *PIPEDA.* An additional challenge is dealing with the substantially similar provinces that are expected to meet certain criteria in order to be deemed substantially similar;[1703] for Alberta and British Columbia, employee information held by provincially regulated organizations is covered by the provincial *AB PIPA* and *BC PIPA* respectively, which is outside the scope of Parliament's legislative authority.[1704]

[1699] *Ibid.* In fact, all businesses operating in Canada and handling personal information that crosses provincial or national borders are subject to *PIPEDA* regardless of the province or territory in which they are based, including provinces with substantially similar legislation. See Privacy Commissioner, "Brief", *supra* note 1672.

[1700] Privacy Commissioner, "Questions", *supra* note 1693.

[1701] *PIPEDA*, *supra* note 1681 at s 12(1).

[1702] Even though there may be fewer *PIPEDA* complaints made by unionized workers because of section 12(1)(a), I assert that it is still necessary to examine labour arbitrations regarding unionized privacy disputes because these workplace privacy cases provide a rich body of case law that provides significant insights about how to best close the electronic surveillance gap.

[1703] *Notice*, *supra* note 1689 at 2388.

[1704] One way to deal with this challenge could be to ask the substantially similar provinces to incorporate the main ideas of the workplace privacy regime into their own legislation within a reasonable period of time, so they too can close the electronic surveillance gap in employment. For example, in *UFCW, Local 401 v Alberta (Information and Privacy Commissioner)*, 2013 SCC 62 at para 41, the Supreme Court of Canada gave the legislature 12 months to make *AB PIPA* compliant as a result of its decision.

It is helpful to consider a couple of examples when understanding the combination of labour and employment and data protection in Canada, and let me assume that we are operating entirely in one province.[1705] If we specifically consider privacy regarding employment information in British Columbia, the federally regulated jurisdiction would be governed by *PIPEDA*, and the provincially regulated jurisdiction would be governed by *BC PIPA*. In contrast, if we specifically consider privacy dealing with employment information in Ontario, the federally regulated jurisdiction would be governed by *PIPEDA*, and the provincially regulated jurisdiction would not be governed by any substantially similar legislation or by *PIPEDA*. As a result, in provinces like Ontario without substantially similar legislation as in Alberta and British Columbia, there would not be the same kinds of legislative workplace privacy protections as provided in *PIPEDA*.

The third challenge that I confronted went beyond the fusion of labour and employment and data protection areas of law—I also had to integrate two competing mindsets pertaining to these fields. More precisely, as I alluded to in Chapter 5, there appears to be a difference in approach when tackling data protection issues compared to labour and employment issues; this struggle is manifested in workplace privacy cases through split decisions and passionate dissents. That is, the data protection realm tends to focus on strict compliance with the rules which are mostly contained in legislation and company policies. Contrarily, the labour relations environment is more inclined to focus on using a contextual approach characterized by several employment principles such as progressive discipline and decision makers giving the employee the benefit of the doubt by conducting a thorough examination of aggravating and mitigating factors and use of remedial authority to award remedies such as reinstatement.

This dissertation requires a synthesis of these opposing mindsets in order to generate ideas that can be used to craft provisions for the new workplace privacy regime. A useful

---

[1705] This is important to note because all businesses operating in Canada and handling personal information that crosses provincial or national borders are subject to *PIPEDA* regardless of the province or territory in which they are based, including provinces with substantially similar legislation. See Privacy Commissioner, "Brief", *supra* note 1672.

tactic is to focus on some of the commonalities of these areas of law that are relevant to privacy and keep them in the back of mind when designing the new workplace privacy regime. These commonalities became apparent during the analyses that took place in Chapters 4 and 5. For example, one commonality is balance and proportionality. In labour and employment disciplinary decisions, a sanction must be proportionate to the misconduct. Likewise, in data protection, there must be a fair balancing of the interests of the parties, and a proportionality analysis makes sure that legitimate interests are necessary and ensures that the intrusiveness of measures corresponds to the degree of risk experienced.

Another commonality is trust. More precisely, there is no question that a core aspect of the employment relationship is trust; when there is a breach of trust, there is a breakdown in the employment relationship. Similarly, trust is critical in a data protection regime because there needs to be trust that any processing will not exceed what is necessary in the circumstances; if it goes beyond what is necessary or is too intrusive, then individuals feel violated and lose trust in the privacy regime.

6.2 The Plan for Designing a New Workplace Privacy Regime

My goal in Chapters 4 and 5 was to extract principles and values from various privacy provisions and workplace privacy cases. The aim was to think as broadly as possible about privacy, consent, and electronic surveillance to take full advantage of the information contained in the privacy provisions and workplace privacy cases. At that stage, the main concern involved identifying and pulling out relevant principles and values. It is now time to convert those ideas into some proposed statutory provisions; this means that there will likely be more ideas than actual proposed provisions, since I will only be providing examples of specific provisions that pertain to closing the electronic surveillance gap in employment.

It is important to ask, however, where to place the proposed provisions: should they be placed in the data protection regime? Or in the labour and employment regime? Since the goal is to create a regime that contains provisions that will effectively close the electronic

surveillance gap in employment, and given that I take myself to be advising Parliament on proposed provisions for a new workplace privacy regime, I can recommend amending either *PIPEDA* or the *Canada Labour Code*. Ultimately, after considering the options and their implications, I have decided to suggest that the proposed provisions be placed in *PIPEDA.* This appears to be the most efficient choice. In particular, it is my contention that since some provisions in *PIPEDA* need to be removed and modified pursuant to my proposals in Chapter 4, and since other provisions need to be created in a structured and well-organized manner, the most effective route is for Parliament to adopt *all* of my ideas that I have proposed in Chapters 4 and 5 and simply place them in *PIPEDA*.

With respect to implementation, since the proposed provisions would only apply in the federally regulated jurisdiction, it may be beneficial to view the new workplace privacy regime as a model for the provinces. It may also be useful to reach out to the provinces in a cooperative manner, and offer to assist them in incorporating some of the ideas into their employment standards and labour relations legislation (or perhaps even future substantially similar data protection legislation, if they prefer) as they act within their legislative authority. Practically speaking, when a policy initiative needs to move forward, the two orders of government usually need to cooperate and promote positive intergovernmental relations.[1706] Thus in the spirit of harmonization, it may be possible to follow in the footsteps of the European Union, which is known for its harmonizing efforts, and convince the provinces to use their legislative authority to promote this important workplace privacy initiative. After all, it can only be beneficial for Canada to present itself as a unified force having consistent privacy protections throughout the country in what is becoming a more *GDPR*-compliant privacy landscape; in order for Canada to continue doing business with EU, it will need to pay attention to the EU's harmonizing pressures and ensure it keeps up with evolving societal values concerning privacy protection.[1707]

[1706] Brown, Bakvis & Baier, *supra* note 1658 at 7.

[1707] Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II")*, C-311/18, EU:C:2020:559. In this case, the Court of Justice of the European Union (Grand Chamber) invalidated the US-EU Privacy Shield program, which was jointly created by the

Therefore, Plan A could be to make proposed provisions and hope for the best, viewing the new workplace privacy regime as a model that could be adopted by provinces in their own way and in their own time when acting within their legislative authority. Plan B could involve being somewhat more proactive to affect more meaningful change by reaching out to provinces and working with them to achieve higher levels of harmonization. I would like to suggest that it would be a shame to not make any efforts to generate at least a couple of creative ideas to support the workplace privacy regime initiative. Thus, a further level could be Plan C, where specific workplace privacy collaborative programs could be created in conjunction with the provinces (perhaps through a partnership between the Ministries of Labour and the Information and Privacy Ombudspersons and Commissioners in Canada), which are supported using the federal spending power as a vehicle to promote Canada's goals.[1708] Perhaps new workplace privacy programs could facilitate the creation of frameworks that resemble the new workplace privacy regime but that can exist in a practical format that meets the needs of organizations in the short-term; these programs could set the stage for future legislative developments in these provinces so that there can be a more gradual closing of the electronic surveillance gap in employment in this regard.

In terms of how to go about creating the proposed provisions to carry out my ideas, I have decided to work with the provisions that already exist in *PIPEDA* where possible, removing and modifying when necessary. However, some ideas that I proposed in Chapters 4 and 5 do not exist anywhere in the legislation; thus, in those situations, I will need to add new provisions to *PIPEDA.*

US Department of Commerce and the European Commission to replace the previously recognized but later abandoned Safe Harbour program.

[1708] Brown, Bakvis & Baier, *supra* note 1658 at 59–60, 119−125.

6.3 Incorporating Previous Guidance by the Privacy Commissioner of Canada

Before proposing the new workplace privacy regime, it is important to review the guidance[1709] that has been provided by the Office of the Privacy Commissioner of Canada and highlight some of its implications for the new workplace privacy regime. Throughout the dissertation, I referred to guidance from the Office of the Privacy Commissioner of Canada as it became relevant to the discussion. I explained that there were several ideas that could be useful for the new workplace privacy regime, ideas that were not expressly included in *PIPEDA's* provisions.

More specifically, I referred to the 2018–2019 Annual Report[1710] when discussing the need to draft rights-based data protections in Theme 1 and also the need to create order-making powers, penalties, and fines in Theme 3. I emphasized the need to use language that encapsulated the dignity/human rights theoretical approach to privacy by incorporating it into the data protection provisions. I also noted that it was necessary to equip the Privacy Commissioner with tools that would allow for the effective enforcement of any findings made under *PIPEDA*.

I mentioned, "Guidelines for Obtaining Meaningful Consent"[1711] in Theme 2 when arguing that employees are not in a position to provide, withhold, or revoke consent in situations involving electronic surveillance, and I suggested that new provisions were required to tackle this issue. I underlined the importance of finding other solutions than

---

[1709] The guidance to which I refer comes from tips, guidelines, guidance documents, and reports of the Office of the Privacy Commissioner of Canada. Some have been created in conjunction with the Information and Privacy Commissioners of Alberta and British Columbia (such as the document discussing a BYOD Program as discussed below).

[1710] Office of the Privacy Commissioner of Canada, "2018-2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act"*(10 December 2019), online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf > [Privacy Commissioner, "2018–2019 Annual Report"].

[1711] Office of the Privacy Commissioner of Canada, "Guidelines for Obtaining Meaningful Consent" (24 May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> [Privacy Commissioner, "Meaningful Consent"].

the consent-based model that would be more appropriate for the employment context, namely the assessment of proportionality.

In addition, I discussed, "Guidance on Covert Video Surveillance in the Private Sector",[1712] in Theme 1 when arguing that "collection" as it currently is described in *PIPEDA* is insufficient for addressing situations involving electronic surveillance in employment, in Theme 2 when pointing out some dangerous aspects of certain *PIPEDA* provisions that could be covert in nature, and also in *Lopez Ribalda*[1713] when discussing covert video surveillance policies. That is, I noted that the way in which collection is described in *PIPEDA* is insufficient when dealing with electronic surveillance issues in the employment context, and something more is required. Further, I stressed that the Office of the Privacy Commissioner of Canada has provided helpful comments related to covert video surveillance; the ideas in this document could be incorporated into the new workplace privacy regime.

I also noted, "Privacy and Social Media in the Workplace",[1714] in Theme 1 when arguing that "collection" as it currently is in *PIPEDA* is insufficient for addressing situations involving electronic surveillance; I also discussed important considerations in respect of social media policies in *Maxam Bulk Services*.[1715] In particular, I argued that the way in which collection is described in *PIPEDA* is insufficient when dealing with electronic surveillance issues in the employment context, and further provisions are required to clearly articulate what takes place in situations involving electronic surveillance.

[1712] Office of the Privacy Commissioner of Canada, "Guidance on Covert Video Surveillance in the Private Sector" (May 2009), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/> [Privacy Commissioner, "Video Surveillance"].

[1713] *López Ribalda and Others v Spain*, Applications 1874/13 and 8567/13, Judgment of the Court (Grand Chamber), 17 October 2019, rev'g Applications 1874/13 and 8567/13, Judgment of the Court (Third Section), 9 January 2018 [*López Ribalda*].

[1714] Office of the Privacy Commissioner of Canada, "Privacy and Social Media in the Workplace" (August 2019), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_41_sn/> [Privacy Commissioner, "Social Media"].

[1715] *Maxam Bulk Services and International Union of Operating Engineers, Local 115 (Lebrun)* (2015), 2015 CarswellBC 2277 (Arbitrator: McConchie) [*Maxam Bulk Services*].

Moreover, there have been some useful protective strategies involving social media that can be added to the new workplace privacy regime.

In referring to various documents concerning mobile devices and in contemplating using a "bring your own device" (BYOD) program[1716] when discussing social media in *Maxam Bulk Services*, I noted that, although this instructive information was not currently reflected in *PIPEDA*, it was very important to include it in the new workplace privacy regime in light of the privacy and security issues that can arise.

Lastly, I also cited the findings in the report, "A Full Year of Mandatory Data Breach Reporting: What We've Learned and What Businesses Need to Know"[1717] in my discussion about legitimate business interests that need to be considered when balancing the interests in *Steel*.[1718] This was essential information to appreciate the context in which the parties were operating; more precisely, it was important to understand the kinds of threats faced by employers (breaches due to unauthorized data accesses), and why it was necessary to protect the legitimate business interests of employers while simultaneously protecting the privacy of employees.

What the foregoing suggests is that, while the Office of the Privacy Commissioner of Canada has generated many interesting ideas about how *PIPEDA* can apply to situations involving electronic surveillance in the employment context, these ideas are not currently included in *PIPEDA*.

[1716] Office of the Privacy Commissioner of Canada, "Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?" (22 July 2015), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/>; Office of the Privacy Commissioner of Canada, "10 Workplace Tips for Protecting Personal Information on Mobile Devices" (January 2011), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_46_dpd/> ; Office of the Privacy Commissioner of Canada, "Contemplating a Bring Your Own Device (BYOD) program?" (August 2015), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/tips_byod/>.

[1717] Office of the Privacy Commissioner of Canada, "A Full Year of Mandatory Data Breach Reporting: What We've Learned and What Businesses Need to Know" (31 October 2019), online (blog): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/blog/20191031/> [Privacy Commissioner, "Breach Reporting"].

[1718] *Steel v Coast Capital Savings Credit Union*, 2015 BCCA 127, aff'g 2013 BCSC 527 [*Steel*].

And in December 2019, when the Office of the Privacy Commissioner of Canada released its 2018–2019 Annual Report[1719] and discussed important topics regarding suggestions for privacy law reform in Canada,[1720] it provided a model preamble and purpose statement for a revamped *PIPEDA* that would appear at the opening of the law and entrench privacy in its proper human rights framework.[1721] Using a rights-based approach to data protection,[1722] the model serves to provide guidance as to the values, principles, and objectives that should shape the interpretation of the law.[1723] The Office of the Privacy Commissioner of Canada proposed wording for *PIPEDA* as follows:

> Proposed wording for PIPEDA
>
> Preamble
>
> WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory;
>
> WHEREAS the right to privacy protects individual autonomy and dignity, and is linked to the protection of reputation and freedom of thought and expression;
>
> WHEREAS privacy is essential to relations of mutual trust and confidence that are fundamental to the Canadian social fabric;
>
> WHEREAS privacy is essential to the preservation of democracy and the full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*;
>
> WHEREAS the current and evolving technological context facilitates the collection of massive quantities of personal data as well as the use of these data, whether in identifiable, aggregate or anonymized forms, in ways that can adversely impact individuals, groups and communities;
>
> WHEREAS the processing of personal data should be designed to serve humankind;

[1719] Privacy Commissioner, "2018–2019 Annual Report", *supra* note 1710 at 11−18.
[1720] *Ibid* at 8–24.
[1721] *Ibid* at 22–23.
[1722] *Ibid* at 12.
[1723] *Ibid* at 22.

WHEREAS responsible processing of personal data can serve public interests such as economic growth, advances in health care and the protection of the environment;

WHEREAS this law protects the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances **and in ways that do not represent surveillance**;

WHEREAS the right to privacy must be balanced with other fundamental rights such as the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

AND WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

Purpose

The purposes of this Act are:

(a) to implement the fundamental right to privacy of all persons in the commercial context through robust data protection that ensures that the processing of data is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals;

(b) to balance privacy rights with the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

(c) to balance privacy rights, where appropriate, with what the public interest requires;

(d) to protect the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances **and in ways that do not represent surveillance**;

(e) to provide individuals with quick and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by organizations with their obligations under this Act.[1724]

[1724] *Ibid* at 22–23 [emphasis added].

When observing the above proposed preamble and purpose section created by the Office of the Privacy Commissioner of Canada, I am encouraged because my ideas for the new workplace privacy regime appear to be in line with this proposed preamble and purpose; I also note that there is a brief mention of surveillance.[1725] In my view, the explicit reference to surveillance provides a useful starting point for discussions regarding surveillance, and I believe that my proposed provisions in the new workplace privacy regime dealing with electronic surveillance in employment have the potential to build on this proposition.

6.4 Examples of Proposed Workplace Privacy Provisions

In this part, I propose some novel provisions for a new workplace privacy regime. These provisions fall under three general categories and involve modifying some existing provisions in Part 1 of *PIPEDA*,[1726] reworking an existing fundamental principle in Schedule 1 of *PIPEDA*,[1727] and creating an innovative fundamental principle in Schedule 1 of *PIPEDA*.[1728]

I will proceed as follows. Under each category, I will first indicate how, in general, I propose to modify or update currently existing provisions, and then I will comment on the nature and effect of the proposed modifications.

6.4.1 Modifying Existing Provisions in Part 1 of *PIPEDA*[1729]

The goal of my proposed changes to Part 1 of *PIPEDA*[1730] is to add, modify, or remove provisions in accordance with my suggestions contained in the analyses throughout the dissertation. There are six main changes in this category. Firstly, I propose adding new definitions that add clarity for supporting new provisions regarding electronic surveillance. Secondly, I propose modifying the purpose provision so that there is

---

[1725] *Ibid.*
[1726] *PIPEDA, supra* note 1681 at ss 2−30.
[1727] *Ibid* at Schedule 1.
[1728] *Ibid*.
[1729] *Ibid* at ss 2−30.
[1730] *Ibid.*

reference to fundamental rights and freedoms, balance, and trust. Thirdly, I propose adding a provision regarding an employee's ability to provide, withhold, or revoke consent and suggest an alternative. Fourthly, I propose removing or modifying specific provisions involving the employment relationship to create a more effective balancing of interests. Fifthly, I propose adding provisions that provide the Privacy Commissioner of Canada with order-making powers and the ability to impose penalties by creating prohibitions, offences, and considerations for imposing fines, and by discussing the effect of the orders. And sixthly, I propose removing the sections that discuss applications to and hearings by the court in order to facilitate the Privacy Commissioner of Canada's order-making powers.

The cumulative effect of these changes is to create a more robust regime that is clearer, more focused, more reflective of the vulnerability of employees in the employment relationships, and better suited to empower the Privacy Commissioner of Canada to carry out a meaningful deterrence approach that is necessary in today's rapidly evolving technological context.

To this end, I first propose adding some definitions to section 2(1) of *PIPEDA*.[1731]

> **Definitions**
>
> **2 (1)** The definitions in this subsection apply in this Part.
>
> ***assessment of proportionality*** means a balancing of interests to determine whether the processing in question is necessary for the purposes of the legitimate interests of employers, except where such interests are overridden by the interests or fundamental rights and freedoms of employees that require data protection.
>
> ***electronic surveillance*** means the systematic creation and/or use of personal data for the investigation or monitoring of actions or communications of one or more persons.

[1731] *Ibid* at s 2(1).

employer means an organization that collects, uses or discloses personal information or conducts electronic surveillance of employees or applicants for employment with the organization, in connection with the operation of a federal work, undertaking or business in line with section 4(1)(b).

excessive means more than necessary.

four temporal dimensions includes

(a) the timeframe in which the electronic surveillance is conducted (ephemeral, across a single span of time, across recurrent spans such as within 24-hour cycles, or scattered across time following a trigger);

(b) the intensity with which the electronic surveillance is conducted (once, repeated, or continuous);

(c) the persistence of consequences of the electronic surveillance (ephemeral because it is limited to observation, short-to-medium term because it is recorded, or long-term or permanent because it is recorded and archived); and

(d) the time period within which the electronic surveillance is applied (the present, real-time use, the past through retrospective use, or the future through prospective or predictive use).

function creep means the repurposing of personal data for new uses without the knowledge of the owner of the personal data.

overly intrusive means causing disruption or adverse effects through being unwelcome or uninvited.

personal data is the same as personal information, which means information about an identifiable individual.

processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

> ***unreasonable electronic surveillance*** means the use of electronic surveillance by an employer that is excessive and/or overly intrusive, and which includes profiling.

Second, in line with my recommendation to refer specifically to fundamental rights and freedoms in the purpose section of the legislation, I propose replacing the current section 3 of *PIPEDA*[1732] with a new section 3. In this new provision I refer to the two main themes that run throughout the entire dissertation that pertain to both data protection and employment, namely balance and trust. Since this part deals with the removal and replacement of a provision, I will list the provision before and after my proposed changes so the differences between the two can be seen.

Before the changes:

> **Purpose**
>
> **3** The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[1733]

After the changes:

> **Purpose**
>
> **3** The purpose of this Part is to protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data, where the focus is on achieving a fair balance of rights and legitimate interests in a manner that enhances trust among the parties involved as well as in the data protection regime.

Third, I propose adding a provision in a new section, 6.1(2), dealing with employee consent and the employment relationship.

[1732] *Ibid* at s 3.
[1733] *Ibid*.

> **Consent in employment**
>
> **6.1 (2)** For the purposes of clauses 4.3 and 4.11 of Schedule 1, employees are hardly ever in a position to freely give, withhold, or revoke consent with respect to the collection, use or disclosure of their personal information, or to electronic surveillance when dealing with employers because of the inherent unequal bargaining power that is present in the employment relationship. Since employees can only give free consent in rare circumstances when no consequences at all are connected to acceptance or rejection of an offer, it is necessary to conduct an assessment of proportionality in most cases.

Fourth, I propose removing section 7.3 of *PIPEDA*[1734] entirely. This section allows employers to collect, use and disclose personal information without the consent of employees if it is to manage or terminate an employment relationship and as long as the employees are informed of the collection, use or disclosure of that information.[1735] Likewise, I propose removing provisions in section 7.4 of *PIPEDA*[1736] that enable organizations to use and disclose employees' personal information for purposes other than those for which the information was collected in any of the circumstances set out in section 7.3 of *PIPEDA.*[1737] Since this part deals with removal of some or all of a provision, I will list the provisions before and after my proposed changes so the differences between the two can be seen.

Before the changes:

> **Employment relationship**
>
> **7.3** In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if
>
> > **(a)** the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and

---

[1734] *Ibid* at s 7.3.
[1735] *Ibid.*
[1736] *Ibid* at s 7.4.
[1737] *Ibid* at s 7.3.

> **(b)** the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.
>
> **Use without consent**
>
> **7.4 (1)** Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.
>
> **Disclosure without consent**
>
> **(2)** Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.[1738]

After the changes:

> **7.3** [Repealed, 2020]
>
> **Use without consent**
>
> **7.4 (1)** Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2).
>
> **Disclosure without consent**
>
> **(2)** Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2).

Fifth, I propose adding a new provision, section 12.3, that enables the Privacy Commissioner of Canada to proactively inspect the premises of an employer, regardless of whether a complaint is made, in order to determine whether the employer is in compliance and to more effectively facilitate its order-making powers. Similarly, I propose adding provisions prohibiting acts of unreasonable electronic surveillance in new sections, 27.2 and 27.3; creating some corresponding fines in new sections, 28.1 and 28.2; listing the considerations when imposing fines in a new section, 28.3; and stating

---

[1738] *Ibid* at ss 7.3−7.4.

the effect of the Privacy Commissioner of Canada's orders in a new section, 28.4. This results in the following new sections:

> **Powers of the Commissioner**
>
> **12.3 (1)** Regardless of whether a complaint is made, the Commissioner may do one or more of the following:
>
> > **(a)** at any reasonable time, enter any premises, other than a dwelling-house, occupied by an employer on satisfying any security requirements of the organization relating to the premises;
> >
> > **(b)** converse in private with any person in any premises entered under paragraph (a) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and
> >
> > **(c)** examine or obtain copies of or extracts from records found in any premises entered under paragraph (a) for the purposes of determining whether the employer is in compliance with this Act, including sections 27.2–27.3.
>
> **(2)** The Commissioner may do one or more of the following:
>
> > **(a)** issue warnings to the employer that certain intended electronic surveillance operations are likely to infringe provisions of this Act, including sections 27.2–27.3;
> >
> > **(b)** order the employer to cease committing acts of unreasonable electronic surveillance of employees;
> >
> > **(c)** order the employer to correct its electronic surveillance practices in order to comply with this Act, and where appropriate, in a specified manner and within a specified period;
> >
> > **(d)** impose a temporary or definitive limitation including a ban on an employer's electronic surveillance operations; and
> >
> > **(e)** impose fines as set out in section 28.1–28.2.
>
> **Prohibition**
>
> **27.2** For the purposes of clause 4.11 of Schedule 1, no employer shall commit acts of unreasonable electronic surveillance of employees.
>
> **27.3** For the purposes of clause 4.11 of Schedule 1, no employer shall conduct mass electronic surveillance, such as the unreasonable electronic surveillance of large numbers of employees in one or more work locations,

for the purposes of manipulating and controlling the employees or their personal data in ways that are detrimental to them.

Offence and punishment

28.1 Every employer that contravenes section 27.2 is guilty of an offence and is liable to a fine not exceeding $100,000, and for a subsequent offence, a fine not exceeding $200,000.

28.2 Every employer that contravenes section 27.3 is guilty of an offence and is liable to a fine not exceeding $10 million.

Considerations for imposing fines

28.3 When deciding whether to impose fines and amounts of fines in each individual case regarding sections 28.1 and 28.2, due regard shall be given to the following considerations:

(a) nature, severity, degree of data sensitivity, and duration;

(b) the intentional or negligent character;

(c) any action taken to mitigate the damage suffered by individuals;

(d) the types of safeguards used;

(e) any relevant previous violations;

(f) the degree of cooperation with the Privacy Commissioner in the current matter;

(g) compliance with previous orders of the Privacy Commissioner;

(h) the size of the organization;

(i) the amount of annual gross profits earned by the organization;

(j) any other aggravating or mitigating factors such as financial benefits gained or losses avoided as a result of the violation.

Effect of the Commissioner's orders

28.4 A decision of the Commissioner becomes executory as a judgment of the Court and has all the effects of such a judgment once filed with the Court.

Sixth, in light of the above newly-created order-making powers and penalties of the Privacy Commissioner of Canada, I propose removing provisions involving applications

to and hearings by the court under sections 14 through to 17.2 of *PIPEDA.*[1739] Since this part deals with the removal of provisions, I will list the provisions before and after my proposed changes so the differences between the two can be seen.

Before the changes:

> **Hearing by Court**
>
> **Application**
>
> **14 (1)** A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, in subsection 5(3) or 8(6) or (7), in section 10 or in Division 1.1.
>
> **Time for application**
>
> **(2)** A complainant shall make an application within one year after the report or notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.
>
> **For greater certainty**
>
> **(3)** For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).
>
> **Commissioner may apply or appear**
>
> **15** The Commissioner may, in respect of a complaint that the Commissioner did not initiate,
>
> > **(a)** apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;
> >
> > **(b)** appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or

[1739] *Ibid* at ss 14−17.2.

(c) with leave of the Court, appear as a party to any hearing applied for under section 14.

Remedies

16 The Court may, in addition to any other remedies it may give,

(a) order an organization to correct its practices in order to comply with Divisions 1 and 1.1;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Summary hearings

17 (1) An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

Precautions

(2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

Compliance agreement

17.1 (1) If the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 or 1.1 or a failure to follow a recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization.

Terms

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part.

Effect of compliance agreement — no application

(3) When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement,

(a) shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and

(b) shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions.

For greater certainty

(4) For greater certainty, a compliance agreement does not preclude

(a) an individual from applying for a hearing under section 14; or

(b) the prosecution of an offence under the Act.

Agreement complied with

17.2 (1) If the Commissioner is of the opinion that a compliance agreement has been complied with, the Commissioner shall provide written notice to that effect to the organization and withdraw any applications that were made under subsection 14(1) or paragraph 15(a) in respect of any matter covered under the agreement.

Agreement not complied with

(2) If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for

(a) an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or

(b) a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result of an application made under paragraph 17.1(3)(b).

> **Time for application**
>
> **(3)** Despite subsection 14(2), the application shall be made within one year after notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.[1740]

After the changes:

> **14** [Repealed, 2020]
>
> **15** [Repealed, 2020]
>
> **16** [Repealed, 2020]
>
> **17** [Repealed, 2020]
>
> **17.1** [Repealed, 2020]
>
> **17.2** [Repealed, 2020]

In my view, the cumulative effect of these changes is that some of the issues that I raised in the problem statement of the Introduction can now be addressed. For example, the proposed definitions provide clarity and help set the stage for the provisions in the next categories that aim to close the electronic surveillance gap. The proposed provision regarding consent, for example, points to the need to use an alternative to a consent model, namely an assessment of proportionality, when dealing with employment relationships in the regime. The changes made to the provisions involving the employment relationship highlight the problem that exists when dealing with power imbalances and goes some way to even out the unequal power distribution between the parties. The proposed prohibitions, offences, and fines help to strengthen the regime by making it more current and responsive to technology, leading to an increased level of trust in the regime.

[1740] *Ibid*.

6.4.2 Reworking Existing Fundamental Principles in Schedule 1 of *PIPEDA*[1741]

Schedule 1 of *PIPEDA* includes Principle 3 in clause 4.3,[1742] which deals with consent. Pursuant to my discussion regarding an employee's ability to provide, withhold, or revoke consent, and in line with my proposed provision 6.1(2), it is my view that the opening of clause 4.3[1743] requires some reworking. The effect of these changes is that it will be clearer from the outset that the employment relationship is unique, and the consent model is in most cases inappropriate in the employment context. In particular, it is necessary to conduct an assessment of proportionality in most cases. Since the focus of this dissertation is on situations involving electronic surveillance, detail regarding how to conduct the assessment of proportionality as it pertains to situations involving electronic surveillance is located in the proposed Principle 11 in clause 4.11.

To this end, I propose modifying the provision by adding eight lines (the last eight lines in underlining) at the end of the opening of clause 4.3 of *PIPEDA*[1744] dealing with consent, to include language that makes it clear that employees are not in a position to provide, withhold, or revoke consent, and it is necessary to conduct an assessment of proportionality in most cases. As mentioned in the newly created definitions above, the assessment of proportionality can be generally understood as a balancing of interests to determine whether the processing in question is necessary for the purposes of the legitimate interests of employers, except where such interests are overridden by the interests or fundamental rights and freedoms of employees that require data protection.

> **4.3 Principle 3 – Consent**
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For

---

[1741] *Ibid* at Schedule 1.
[1742] *Ibid* at Schedule 1, cl 4.3.
[1743] *Ibid*.
[1744] *Ibid*.

> example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information. Furthermore, employees are hardly ever in a position to freely give, withhold, or revoke consent when dealing with employers because of the inherent unequal bargaining power that is present in the employment relationship. Since employees can only give free consent in rare circumstances when no consequences at all are connected to acceptance or rejection of an offer, seeking consent from employees or expecting that they may be able to withhold or revoke consent is often impractical. It is necessary to conduct an assessment of proportionality in most cases.

6.4.3 Creating a New Fundamental Principle in Schedule 1 of *PIPEDA*[1745] Entitled *Electronic Surveillance: Working Within Reason*

Finally, I propose adding a new fundamental principle in Schedule 1 of *PIPEDA*[1746] entitled *Electronic Surveillance: Working Within Reason*. The goal of this new fundamental principle is to create simple, fundamental provisions that are clear and easy to understand. The provisions I propose are a combination of all my suggestions stemming from my analyses throughout Chapters 4 and 5, which have been boiled down into 11 foundational points. The main points involve: (1) duties of care, loyalty, and confidentiality; (2) privacy by design; (3) balanced policies and procedures; (4) creating an ethical work culture as part of a data protection program; (5) data impact risk assessments when dealing with new technologies; (6) assessments of proportionality to determine if electronic surveillance is can be conducted/can continue to be conducted; (7) social media; (8) mobile digital devices; (9) electronic communications; (10) video surveillance; and (11) situations involving electronic surveillance outside the workplace.

[1745] *Ibid* at Schedule 1.
[1746] *Ibid.*

The effect of these changes is to create a more meaningful set of foundational principles that can be used to close the electronic surveillance gap in the employment context, by setting out what I believe are essential considerations that should be addressed when dealing with situations involving electronic surveillance in employment.

Since Principle 11 in clause 4.11 has been placed in Schedule 1 of *PIPEDA*[1747] it is important to note the effect of the proposed provisions by looking to section 5 of *PIPEDA*:[1748]

> **Compliance with obligations**
>
> **5 (1)** Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.
>
> **Meaning of should**
>
> **(2)** The word should, when used in Schedule 1, indicates a recommendation and does not impose an obligation.[1749]

To that end, for the purposes of Principle 11 in clause 4.11, it follows that employers would have to comply with the proposed obligations and consider the word, "should" to be a recommendation. The Principle includes 11 subsidiary sections, as set out below.

> **4.11 Principle 11 — Electronic Surveillance: Working Within Reason**
>
> Employees are in a vulnerable position and are at risk of being exploited by employers due to the inherent unequal bargaining power that is present in the employment relationship. Since employees are not in a position to freely provide, withhold, or revoke consent in most situations involving electronic surveillance, seeking consent from employees or expecting that they may be able to withhold or revoke consent is often impractical. Given the consequences associated with excessive and/or overly intrusive monitoring inside and outside the workplace, a fair balance must be achieved between the parties, so that the legitimate business interests of employers and the fundamental rights and freedoms of employees are equally respected, and so that trust can be enhanced among the parties as well as in the data protection regime.

[1747] *Ibid.*
[1748] *Ibid* at s 5.
[1749] *Ibid*.

4.11.1

Employers must, while meeting business goals, meet the following duties of care, loyalty, and confidentiality to employees:

> **(a)** Duty of care means refraining from engaging in function creep by clearly and distinctly stating existing purposes for electronic surveillance and any additional desired purposes, protecting the personal data of employees generated from acts of reasonable electronic surveillance by using appropriate safeguards, and being prudent when making decisions to conduct electronic surveillance, working with surveillance reports, and imposing discipline as a result of the information revealed in the reports;
>
> **(b)** Duty of loyalty means faithfully enabling employees to perform their work with dignity and self-respect and without being subject to unreasonable electronic surveillance, meeting legitimate business interests without using employees' personal data to their detriment in a way that causes physical, psychological, financial, or reputational harm (while discipline does not in itself constitute harm as contemplated in this part, any discipline resulting from electronic surveillance must be imposed in good faith), and faithfully making efforts to give employees the benefit of the doubt and not jump to conclusions when engaging with electronic surveillance technologies; and
>
> **(c)** Duty of confidentiality means not disclosing or sharing employees' personal data with anyone unless it is aligned with the employer's duties of care and loyalty (keeping in mind requirements to obey the law, protect vital interests of employees or others, protect public interests, and perform legal or contractual obligations), refraining from engaging in profiling involving any of the prohibited grounds of discrimination as set out in the *Canadian Human Rights Act*, RSC, 1985, c H-6, s 3, and aspiring to ensure that employees' sensitive personal data that surfaces when conducting electronic surveillance is handled with meticulous safekeeping and is not disclosed, sold, or shared.

4.11.2

Employers must at all times make data protection the default and consider: the nature and extent (including the four temporal dimensions and degree of intrusion), purposes, and consequences of the electronic surveillance; the impact on employees' rights and freedoms; and the necessary physical, organizational, and technological safeguards to address the risks. By default, only personal data that is necessary for each specific purpose can be subject to electronic surveillance, and only designated individuals who need to know the information are to have access to it. The principles of privacy by design

apply to electronic surveillance in the employment context: be proactive and preventative; set the data protection of employees as the default at all times; embed privacy protection into the design of the organization's policies and procedures; strive to achieve win-win outcomes for the parties; provide lifetime employee protection; have transparent rules; and create clear and understandable expectations so employees have a firm grasp of the rules.

4.11.3

To build and maintain trust in the employment relationship, employers must create balanced policies and procedures regarding electronic surveillance in the workplace. While the types of policies and procedures may vary depending on the circumstances, employers must ensure that the policies and procedures are attentive to the needs of both parties, transparent, and clearly communicated during training sessions. For example, some policies can address the needs of employees by clearly informing employees about details concerning the monitoring; data retention; attempts to minimize the intrusion; and the individuals who have access to the data. Correspondingly, some policies can protect employers' legitimate interests such as protecting client or employee data and other corporate interests such as corporate information, reputation, and intellectual property by explaining: company rules; disciplinary consequences of noncompliance and breaches of trust; as well as expectations for employees who work in positions of authority, work autonomously, or work in positions requiring special trust.

4.11.4

Employers have a legitimate business interest in strengthening their data protection programs and must create policies and procedures to achieve this goal. While the policies and procedures may vary depending on the circumstances, employers must ensure that they are creating social norms that are aimed at preventing employee unethical misconduct such as unauthorized data accesses and disclosures. Employers should use several strategies to build and maintain an ethical workplace culture, such as: creating a code of conduct; using effective recruitment and promotion techniques that value managers and employees who have integrity; developing ethical decision-making policies and procedures; creating whistleblower policies and procedures; operating with zero-tolerance company rules; and treating all instances of noncompliance equally.

4.11.5

When using new technologies, and taking into account the considerations in clause 4.11.2, where a type of electronic surveillance is likely to result in a high risk to the rights and freedoms of employees, employers must first conduct an assessment of the impact of the electronic surveillance on the protection of personal data in order to decide if the proposed electronic

surveillance is reasonable. The assessment must describe and document: the proposed electronic surveillance operations, the purpose, and the legitimate interest pursued; an assessment of the necessity and proportionality of the electronic surveillance operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the physical, technological and organizational safeguards used to address the risks. Where it is concluded that the electronic surveillance would be unreasonable, employers must not conduct unreasonable electronic surveillance of employees.

4.11.6

Employees are hardly ever in a position to freely give, withhold, or revoke consent when dealing with employers in situations involving electronic surveillance because of the inherent unequal bargaining power that is present in the employment relationship. Therefore, it is necessary to conduct an assessment of proportionality in most cases. Taking into account the considerations in clause 4.11.2, employers must ensure that any electronic surveillance operations are necessary for a legitimate business purpose and in compliance with principles of proportionality. To conduct the assessment of proportionality, employers must first determine prior to the deployment of any monitoring tool: whether all the data is necessary; whether the electronic surveillance outweighs the general privacy rights of employees; and what measures must be taken to ensure that any privacy violations are limited to the minimum necessary. Employers must have policies and procedures to maintain proportionality at all times and perform regular assessments of proportionality. After each assessment, where it is concluded that the electronic surveillance would be unreasonable and cannot be modified to be reasonable, employers must not begin or stop conducting such unreasonable electronic surveillance. Although the default approach involves conducting an assessment of proportionality, there may be rare circumstances where the parties identify that it is appropriate for them to agree to the joint creation of further data protections that apply to electronic surveillance in their specific workplace, keeping in mind that there must be free consent, adequate safeguards, and recognition that it is not possible to restrict the privacy of employees to zero. Ultimately, when asking whether it is possible to conduct electronic surveillance or continue to conduct electronic surveillance, employers will most likely conduct an assessment of proportionality, with rare exceptions that include one or more of the following: employee consent; performing legal or contractual obligations; protecting vital interests of individuals; or acting in the public interest.

4.11.7

Employers must have social media policies and procedures that clearly state that they will not require or request employees or applicants to disclose social media usernames or passwords, access personal social media in their

presence, or provide any personal information from their social media accounts (and they will not impose any discipline when employees or applicants refuse to do so). Employers must not abuse electronic surveillance power by conducting unreasonable ubiquitous surveillance from outside the workplace to make disciplinary decisions inside the workplace. Employers must clearly articulate their expectations regarding social media use in the workplace: the differences between work and personal accounts; the kind of corporate information that must be kept confidential or undisclosed; the types of social media sites that are appropriate to use in the workplace; the language and behaviour that is expected of employees when they go online given the public nature of social media, the realities of the online environment, and how ubiquitous surveillance can be used to harm the reputations of clients and both parties; and the consequences of noncompliance. Employers must clearly stipulate that it is unacceptable to engage in the online harassment of coworkers while on-duty or off-duty, using any device. Employers must conduct an assessment of proportionality pursuant to clause 4.11.6 when monitoring the social media use of employees during work on work devices, notify them, and explain the details of the monitoring, taking into account clause 4.11.2.

4.11.8

Employers must clearly explain in Bring Your Own Devices policies and procedures their expectations when employees use their own digital devices in the workplace. Employers must notify and explain what electronic surveillance techniques are used that can affect the data stored on employees' personal digital devices, and confirm that they will not access the personal containers/compartments of partitioned devices. Where Mobile Device Management is used to connect to the corporate network, employers must not engage in unreasonable remote manipulations, recording, or tracking of the device. Employers must conduct an assessment of proportionality pursuant to clause 4.11.6 when attempting to monitor online activity, communications, or any data stored on the personal digital devices of employees, taking into account clause 4.11.2. Employers should also: assess privacy risks and threats; provide training to employees; mitigate risks by partitioning the device into containers/compartments; create storage and retention policies; use encryption for devices and communications; protect against software vulnerabilities; manage apps by having a list of approved apps and state how apps are installed, updated, and removed; use effective authentication and authorization procedures for devices, users, and containers/compartments; protect against malware; and create an incident management process.

4.11.9

Employers must create clear policies and procedures regarding the electronic surveillance of electronic communications in the workplace using

their equipment, which can be on corporate digital devices, through the corporate network, and stored on corporate servers or other gear. Employers must conduct an assessment of proportionality pursuant to clause 4.11.6 when attempting to monitor communications at work, taking into account clause 4.11.2. Before conducting the electronic surveillance, employers must notify employees about the monitoring and its implementation. Employers must explain the details of the monitoring, including the particular data that the employer wishes to access, such as specific content or metadata involving the communications.

4.11.10

Employers must take special care with respect to video surveillance, and be particularly discerning when deciding on the limited number of designated individuals who have access to the data, and data retention rules. Employers must conduct an assessment of proportionality pursuant to clause 4.11.6 when attempting to use video surveillance at work, taking into account clause 4.11.2. Before conducting video surveillance, employers must notify employees about the monitoring and its implementation. Employers must explain the details of the monitoring, including the kinds of images that may be captured using the technology. Covert video surveillance of an employee is viewed as a considerable intrusion because it may involve recording and reproducing documentation about an employee's conduct at work, which is a place where the employee has to be and cannot evade; since it is an extremely privacy-invasive form of technology, it must be considered only in the most limited cases. Employers must not conduct continuous covert video surveillance on all employees during all working hours—there first must be reasonable suspicion (that is clearly defined and supported with evidence that the relationship of trust has been broken), and special attention paid to using the least intrusive means of obtaining the information rather than targeting all employees for long periods of time. Employers must have policies stipulating: the criteria that must be met before covert video surveillance is undertaken; the secure storage, retention, and destruction requirements; and the procedures for dealing with third party information. Employers should document details relating to any instances of video surveillance and enter into a service agreement with private investigators hired to conduct the surveillance. Employers must not use as the sole basis of employment decision-making video analytics, predictive analytics, or automated decisions that are made by artificial intelligence. Employers must not use a facial recognition service on employees inside the workplace.

4.11.11

Employers must create policies and procedures regarding electronic surveillance that is conducted outside the workplace, and confirm that this type of electronic surveillance is only conducted on employees in the rare cases where it is necessary because there is reasonable suspicion of off-duty

> misconduct (that is clearly defined and supported with evidence that the relationship of trust has been broken). When deciding whether to commence electronic surveillance outside the workplace, employers must give employees the benefit of the doubt and attempt to understand their version of the story before hastily commencing electronic surveillance. Employers must conduct an assessment of proportionality pursuant to clause 4.11.6 when attempting to use electronic surveillance outside the workplace, taking into account clause 4.11.2. The policies and procedures must stipulate: how decisions are made regarding the details of the monitoring; the types of technologies that are used; the kinds of third parties that are engaged; and the goal to constantly perform checks to ensure that the monitoring remains necessary and proportionate. Where employers conduct the electronic surveillance, upon receiving the surveillance report, employers must carefully examine the electronic surveillance report, scrutinize the sources in the surveillance report (including their motives), and share the information with only a minimal number of designated individuals who need to know the information. When deciding to act on the report, employers must take care to observe contractual provisions and procedures to ensure the imposition of discipline in good faith. When covert video surveillance is conducted outside the workplace, employers must comply with relevant parts of clause 4.11.10. Employers must not use a facial recognition service on employees outside the workplace.

Principle 11 in clause 4.11 touches on the following topics, and does so in order to close the electronic surveillance gap: (1) duties of care, loyalty, and confidentiality; (2) privacy by design; (3) balanced policies and procedures; (4) creating an ethical work culture as part of a data protection program; (5) data impact risk assessments when dealing with new technologies; (6) assessments of proportionality to determine if electronic surveillance is can be conducted/can continue to be conducted; (7) social media; (8) mobile digital devices; (9) electronic communications; (10) video surveillance; and (11) situations involving electronic surveillance outside the workplace. By addressing these issues, Principle 11 in clause 4.11 makes it clear that there can be a legislative response to the main technological concerns that arise when employers and employees are confronted with surveillance and privacy issues in the digital era. With these proposed provisions under Principle 11 in clause 4.11, there will no longer be an absence of appropriate legal provisions to regulate employers' electronic surveillance of employees both inside and outside the workplace. The direction provided allows for a better balancing of interests, namely the privacy rights of employees with the legitimate business interests of employers.

6.5 Conclusion

In Chapters 4 and 5, I proposed ideas for incorporating principles and values extracted from the privacy provisions and workplace privacy cases into the proposed workplace privacy regime to close the electronic surveillance gap in employment.

In this Chapter 6, I have proposed concrete changes to *PIPEDA* based on the principles and values identified in Chapters 4 and 5. More specifically, I did four things. First, I discussed some of the challenges that I encountered when considering how to create a new workplace privacy regime. I discussed the temptation of wanting to create provisions that fell into each of the areas of law that are relevant to privacy simultaneously, but I also noted that this was impractical and that it was necessary to focus on one or two areas (data protection and labour and employment). I also discussed the challenges raised by Canadian federalism and other jurisdictional issues when dealing with the creation of the workplace privacy regime and noted that it was important to understand the inner workings of the chosen areas of law when deciding how to proceed. Lastly, I discussed the challenges involved with the fusion of data protection and labour and employment mindsets, and concluded that it was necessary to integrate the different approaches and observe commonalities in order to more effectively create provisions for the workplace privacy regime.

Second, I discussed the transition from divergent idea generation, which took place in Chapters 4 and 5, to the converging of ideas in this Chapter. I also decided where to place the provisions, namely in the data protection regime. Lastly, I created a strategy for implementing the plan for the workplace privacy regime.

Third, I reflected on previous guidance provided by the Office of the Privacy Commissioner of Canada. More specifically, I referred to several guidance documents that I discussed throughout the dissertation and argued that much of that valuable information was not currently included in *PIPEDA*. I stressed the importance of finding ways to incorporate the information into the new workplace privacy regime.

And fourth, I provided some examples of proposed provisions that could form part of a new workplace privacy regime by modifying selected existing provisions in Part 1 of *PIPEDA*,[1750] reworking a fundamental principle in Schedule 1 of *PIPEDA*,[1751] and creating new provisions in a fundamental principle entitled, *Electronic Surveillance: Working Within Reason*, in Schedule 1 of *PIPEDA*.[1752] It is my hope that the cumulative effect of my proposed changes to *PIPEDA* goes some way towards effectively closing the electronic surveillance gap in the employment context.

[1750] *PIPEDA*, *supra* note 1681 at ss 2−30.
[1751] *Ibid* at Schedule 1.
[1752] *Ibid*.

Chapter 7

7 Conclusion

This dissertation has argued that there is an electronic surveillance gap in the employment context, a gap that is best understood as an absence of appropriate legal provisions to regulate employers' electronic surveillance of employees both inside and outside the workplace.

Canada is already falling behind other progressive jurisdictions with respect to privacy protection. Current privacy provisions in *PIPEDA* are insufficient and do not match the level of sophistication of those in other jurisdictions, especially those of the European Union. Moreover, Canadian data protection provisions that apply in the employment context are inconsistent and confusing, and this creates an unfair patchwork of protections for Canadians: Canadian employees enjoy different data protections depending on the province in which they are located, their unionization status, and what sector—public or private—they are part of. This dissertation has demonstrated that there are significant gaps in Canada's privacy regime when it comes to providing the necessary protections for employees against employers' unreasonable electronic surveillance. There are currently no provisions in place in *PIPEDA* or elsewhere that can effectively deal with employment situations where it is necessary to balance the interests of employers who need direction on how to achieve their legitimate business goals using electronic surveillance, within reasonable limits, and employees who need protection so they can do their jobs without being monitored in excessive or overly intrusive ways.

If *PIPEDA* is to be the floor of privacy protections,[1753] then it must be updated to account for the technological advances that have taken place since its inception in 2000. The current threshold of privacy protections is too low in large part because protections regarding electronic surveillance are nowhere to be found in *PIPEDA*. While it is understandable that *PIPEDA* was not equipped with the provisions to close the electronic

[1753] Notice (Industry Canada), (2002) C Gaz I 2388 (Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council) at 2387 [*Notice*].

surveillance gap when it was created in 2000, it is no longer acceptable to stand by and ignore the numerous calls for change made by the Privacy Commissioner of Canada (and also the Information and Privacy Ombudspersons and Commissioners from across Canada).[1754] Not only does the law need to catch up with social and technological advances, but it also needs to become more nimble and flexible if it is to be able to adapt to the rapid technological advances that are very likely to take place in the near future.

The main goal of this dissertation has been to diagnose how and why the electronic surveillance gap has arisen, and to offer some proposals for how to close that gap in the Canadian employment context. This dissertation has sought to identify and determine how the principles and values manifested in the selected privacy provisions and workplace privacy cases can be used to close the electronic surveillance gap in a manner consistent with Canada's legal system.

In my view, current approaches to the electronic surveillance gap, to the extent that they recognize that such a gap exists, do not provide protections that are sufficient to meaningfully address the electronic surveillance gap in Canada in a way that is consistent with Canadian legal and social values. This dissertation has suggested that, through the synthesis of social theories involving surveillance and privacy, together with in-depth analyses of privacy provisions and workplace privacy cases, a new and better workplace privacy regime can be designed.

To that end, I proposed various novel legislative provisions in Chapter 6, and argued that these provisions could better protect the dignity and self-respect of employees, while still

---

[1754] Office of the Privacy Commissioner of Canada, "2018-2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*" (10 December 2019) at 2, online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf > [Privacy Commissioner, "2018–2019 Annual Report"]; Office of the Privacy Commissioner of Canada, "Canada's Access to Information and Privacy Guardians Urge Governments to Modernize Legislation to Better Protect Canadians" (6 November 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/>; Office of the Privacy Commissioner of Canada, "Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners" (1−2 October 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191106/>.

allowing employers to responsibly use their electronic surveillance power to achieve their legitimate business goals. I argued that the proposed provisions could promote enhanced trust in the employer-employee relationship, minimize the chilling effects that electronic surveillance can have on employee morale, and go some way towards ensuring that gainful employment can provide a sense of meaning, dignity, and self-respect to employees, free from concerns about inappropriate employer intrusions into their private lives.

More specifically, the introductory Chapter 1 set out the problem to be addressed, namely the electronic surveillance gap in employment. It explained the focus and justification for the dissertation, as well as the dissertation's objective. Chapter 1 also described the research question, hypotheses, methodology, and the theoretical framework used in this dissertation.

Chapter 2 explored surveillance theories from the perspective of a capitalist surveillance framework. In it I argued that there is a serious potential for employers to exploit their panoptic electronic surveillance powers and take advantage of their vulnerable employees using excessive and overly intrusive electronic surveillance. I contended that employers had the potential to take advantage of the electronic surveillance technologies indirectly with ubiquitous surveillance regarding off-duty conduct, and also directly in the workplace with electronic surveillance of the workplace premises concerning on-duty conduct. It was important to study social theories of surveillance in order to understand the potential for the abuse of surveillance power, develop a deeper sense of the problem of the electronic surveillance gap in employment, and generate unique insights when performing the legal analyses of the privacy provisions and the workplace privacy cases. In my view, a careful reflection of these informative social theories of surveillance led to the generation of more creative ideas when crafting the proposed workplace privacy regime.

Chapter 3 investigated privacy theories from a dignity/human rights perspective of privacy. Given that this dissertation involved socio-legal analyses regarding workplace privacy in light of electronic surveillance technology, it was necessary to understand both

surveillance and privacy from a theoretical point of view. To that end, Chapter 3 investigated several privacy theories and defended the claim that it was necessary to proceed with a dignity/human rights approach when answering the question, "What is privacy?" I argued that the dignity/human rights approach to privacy provided the best understanding of privacy and allowed for a purposive interpretation of the value of privacy that did not leave the most vulnerable citizens behind. I argued that this flexible approach could enable the creation of incremental modifications to the law while adapting to an evolving society and achieving appropriate balances between competing interests. I maintained that the approach was fitting for tackling issues associated with rapid technological change. It was important to study social theories of privacy in order to better understand what was in need of protecting. In my view, looking through the lens of the dignity/human rights approach enabled the creation of protective provisions that could more effectively close the electronic surveillance gap in the employment context.

Chapter 4 examined selected privacy provisions from Canada, the United States, and the European Union. There was a mix of privacy provisions of the various jurisdictions in each theme. I noted the provisions that fell within each of the three themes, analyzed the provisions of each theme, and set out my ideas for incorporating the detected principles and values into the proposed workplace privacy regime to close the electronic surveillance gap in employment. These ideas stemmed from my discussion of the implications for the new workplace privacy regime. What I found was a series of gaps in Canada's privacy regime, and I borrowed several ideas from other jurisdictions in an attempt to fill those gaps.

Chapter 5 examined six selected workplace privacy cases from Canada, the United States, and the European Union. I described each workplace privacy case, analyzed the case, and indicated how I proposed to incorporate the principles and values thereby identified into the proposed workplace privacy regime, all in attempt to close the electronic surveillance gap in employment. These analyses enabled me to isolate essential principles and values that could lead to novel ideas for the creation of the new workplace privacy regime. Again, the goal was to generate different ideas that would result in a textured foundation

on which to draw for the purposes of creating effective proposed provisions for the new workplace privacy regime.

Chapter 6 was the most complicated Chapter in the dissertation. In it I proposed provisions for the new workplace privacy regime. The Chapter had four main parts. In the first part of the Chapter, I discussed some of the challenges that I encountered when creating a new workplace privacy regime. I then discussed the temptation of wanting to create provisions that fell into each of the areas of law that are relevant to privacy simultaneously, but I also noted that this was impractical and that it was therefore better to focus on one or two areas (data protection and labour and employment). I also discussed the challenges raised by Canadian federalism and other jurisdictional issues when dealing with the creation of the workplace privacy regime, and noted that it was important to understand the inner workings of the chosen areas of law when deciding how to proceed. Lastly, I discussed the challenges involved with the fusion of data protection and labour and employment mindsets, and concluded that it was necessary to integrate the different approaches and observe commonalities in order to more effectively create provisions for the workplace privacy regime.

In the second part of Chapter 6, I discussed the transition from divergent idea generation, which took place in Chapters 4 and 5, to the converging of ideas, which took place in Chapter 6, so that the ideas could be specifically focused on selected issues. I also decided where to place the provisions, namely in data protection. Lastly, I created a strategy for implementing the plan for the workplace privacy regime.

In the third part of Chapter 6, I reviewed the previous guidance provided by the Office of the Privacy Commissioner of Canada with an eye to incorporating the ideas into the new workplace privacy regime. More specifically, I highlighted the several guidance documents to which I referred throughout the dissertation and argued that much of that valuable information was not included in *PIPEDA*. I stressed the importance of finding ways to incorporate the information into the new workplace privacy regime.

In the fourth and final part of Chapter 6, I provided some examples of proposed provisions that could form part of a new workplace privacy regime under three categories

involving modifying selected existing provisions in Part 1 of *PIPEDA,*[1755] reworking an existing fundamental principle in Schedule 1 of *PIPEDA,*[1756] and creating a new fundamental principle, Principle 11 in clause 4.11, entitled, *Electronic Surveillance: Working Within Reason,* in Schedule 1 of *PIPEDA.*[1757] It is my belief that these are the kinds of provisions needed to effectively close the electronic surveillance gap in the employment context.

The Office of the Privacy Commissioner of Canada recently highlighted one of the main issues discussed in this dissertation. In its 2018–2019 Annual Report, it stated the following:

> Our laws have simply not kept pace with the reality in which they operate. Our reality is now one in which new business models that rely on personal information emerge daily, and the stockpiling of personal information is increasingly seen as a competitive advantage. It is a reality in which individuals, businesses and government are all seeking to harness the benefits of technology, often without a full understanding of the risks it poses. This increased reliance on technology, combined with the ease with which information flows across borders and changes hands makes it difficult for individuals to know if they are dealing with a human or a robot, an entity in Canada or elsewhere, or the public or private sector. In this complex digital environment, what is clear is that our privacy laws need to be reflective of the current times, and more forcefully assert protections for the rights of Canadians. Now is the time for action.[1758]

Not only is it important for the law to stay current when it comes to technology, but it is also essential that the law be able to protect essential Canadian values, including the dignity and self-respect of employees in the employment context. As Dickson C.J. noted:

> Work is one of the most fundamental aspects in a person's life, providing the individual with a means of financial support and, as importantly, a contributory role in society. A person's employment is an essential component of his or her sense of identity, self-worth and emotional well-being. Accordingly, the conditions in which a person works are highly

---

[1755] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 at ss 2−30 [*PIPEDA*].
[1756] *Ibid* at Schedule 1.
[1757] *Ibid*.
[1758] Privacy Commissioner, "2018–2019 Annual Report", *supra* note 1754 at 21.

> significant in shaping the whole compendium of psychological, emotional and physical elements of a person's dignity and self-respect.[1759]

Part of the goal of this dissertation has been to reconcile recent (and future) social and technological advances in electronic surveillance technology with the need to protect the privacy interests and dignity of individuals in private workplaces. This dissertation is not without limitations, however. The most important limitation is the fact that it has focused almost exclusively on the labour and employment context. This was by design, though, since the workplace context is one of the most important places in which the right to privacy comes into conflict with other competing interests, such as the interest of employers in ensuring that employees are in fact doing what they were hired to do and are using technology in ways that do not harm their employers. However, while the findings and recommendations made here can serve as a useful starting point for research in other contexts in which privacy concerns arise, specific research tailored to the context in question would be needed to close the electronic surveillance gap in those other contexts.

Moving forward, I anticipate that future research in this area will involve a shift away from the workplace, where goods and services are produced, to the consumer context, where goods and services are received and consumed. There are growing concerns about potential abuses of surveillance power by large technology companies; one example involves social media companies using monitoring and persuasive technology tools to monopolize attention and manipulate users.[1760] Additionally, I believe that an important future project would be to investigate the possibility of recognizing a right to privacy and freedom from unreasonable electronic surveillance throughout Canada. This would have to be done in a way that is consistent with Canadian values and also practical given the

---

[1759] *Reference Re Public Service Employee Relations Act (Alta)*, [1987] 1 SCR 313 at para 95, 1987 CarswellAlta 705 (SCC) [*Alberta Reference*].

[1760] City Arts & Lectures, "City Arts & Lectures presents Your Undivided Attention: Persuasive Technology: Tristan Harris in conversation with Jacob Ward" (30 April 2020), online (video): *YouTube* <https://www.youtube.com/watch?v=0TZKOuQLMfM>. See also Tristan Harris, Tim Wu & Aza Raskin, "Episode 16: When Attention Went on Sale" (28 April 2020), online (podcast): *Center for Humane Technology: Your Undivided Attention* <https://humanetech.com/>; Cennydd Bowles, *Future Ethics* (United Kingdom, NowNext Press, 2018) at 35−59; (Roger McNamee, *Zucked* (New York: Penguin Press, 2019) at 178–240; Nir Eyal with Ryan Hoover, *Hooked* (New York: Portfolio/Penguin, 2014) at 15−178.

challenges I referred to in Chapter 4, Theme 1, involving *Bill S-21 (Privacy Rights Charter)*.[1761] Lastly, other topics that touch on tensions between surveillance and privacy might involve the need for data protection in the creation of smart cities such as the now-defunct Google Sidewalk Labs in Toronto,[1762] and the privacy rights that are implicated when crossing international borders with digital devices.[1763]

In designing the proposed workplace privacy regime, I have drawn on the instructive work of Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, who is known for creating the principles of Privacy by Design.[1764] I have tried to design a workplace privacy regime that is both proactive and preventative; that sets data protection as the default; embeds privacy protection into the design of the regime; that creates balance and consequent win-win outcomes for the parties; provides lifetime protection for employees; insists on transparency of rules and requirements; and that creates understandable expectations for Canadians that can be used in the employment context.[1765] It is my hope that the proposed provisions for a new workplace privacy regime will better balance the interests of Canadians in ensuring that workplaces that are free from excessive and overly intrusive employer oversight with the needs of employers to protect client and employee information, reputation, property, corporate trade secrets,

---

[1761] Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess, 37th Parl, 2001 (first reading 13 March 2001, dropped from the Senate Order Paper in 2002) [*Bill S-21 (Privacy Rights Charter)*]; The Standing Senate Committee on Social Affairs, Science and Technology, "Report of the Committee" (14 December 2001), online: *Senate of Canada* <https://sencanada.ca/Content/SEN/Committee/371/soci/rep/rep13dec01-e.htm>.

[1762] Juan-Louis Suarez, "Sidewalk Labs Dumping the Quayside Development Might Signal a Bright Future for Toronto" (15 May 2020), online: *The Star* <https://www.thestar.com/opinion/contributors/2020/05/15/sidewalk-labs-dumping-the-quayside-development-might-signal-a-bright-future-for-toronto.html>; Leyland Cecco, "Google Affiliate Sidewalk Labs Abruptly Abandons Toronto Smart City Project" (7 May 2020), online: *The Guardian* <https://www.theguardian.com/technology/2020/may/07/google-sidewalk-labs-toronto-smart-city-abandoned>.

[1763] Sophia Cope et al, "Digital Privacy at the U.S. Border: Protecting the Data on Your Devices" (December 2017), online (pdf): *Electronic Frontier Foundation* <https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf>; Matthew Braga, "What happens when a Canadian border agent asks to search your phone?" (3 March 2017), online: *CBC* <https://www.cbc.ca/news/technology/border-phone-laptop-search-cbsa-canada-cbp-us-1.4002609>.

[1764] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles" (January 2011), online (pdf): *Office of the Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

[1765] *Ibid*.

and confidential information. If this is achieved, then I believe that we will have gone a long way toward effectively closing the electronic surveillance gap in the employment context.

Bibliography

LEGAL INSTRUMENTS

Act Respecting Labour Standards, CQLR c N-1.1.

An Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1.

Bill 38, *Personal Information Protection Act*, 4th Sess, 37th Leg, British Columbia, 2003 (assented to October 23, 2003), SBC 2003, c 63.

Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess, 37th Parl, 2001 (first reading 13 March 2001, dropped from the Senate Order Paper in 2002).

Breach of Security Safeguards Regulations (SOR/2018-64).

Cal Civ Code, 3 CIV 1.81 (2000).

Cal Const art I.

California Consumer Privacy Act of 2018, 3 CIV 1.81.5 (2018).

Cal Lab Code (2012).

Canadian Human Rights Act, RSC, 1985, c H-6.

Canada Labour Code, RSC, 1985, c L-2.

Canada SOR/2004-219.

Canada SOR/2004-220.

Canada SOR/2003-374.

Canadian Charter of Rights and Freedoms, s 7, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982*(UK),1982, c 11.

Canadian Human Rights Act, RSC, 1985, c H-6.

Charter of Human Rights and Freedoms, CQLR c C-12.

Civil Rights Act of 1964 Pub L, 88–352, 78 Stat 241.

Constitution Act, 1867 (UK), 30 & 31 Vict, c 3 s 91, reprinted in RSC 1985, Appendix II, No 5.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5 (1950).

Criminal Code, RSC, 1985, c C-46.

Digital Privacy Act, SC 2015, c 32.

EC, *Decision 2002/2/EC Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, [2002] OJ, L002/0013.

EC, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] OJ, L281/0031.

EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L119/1.

Employment Standards Act, 2000, SO 2000, c 41.

Employment Standards Act, RSBC 1996, c 113.

Employment Standards Act, RSPEI 1988, c E-6.2.

Employment Standards Act, SNB 1982, c E-7.2.

Employment Standards Act, SNWT 2007, c 13.

Employment Standards Act, RSY 2002, c 72.

Employment Standards Code, RSA 2000, c E-9.

Highway Traffic Act, RSO 1990, c H.8.

Industrial Relations Act, RSNB 1973, c I-4.

Labour Act, RSPEI 1988, c L-1.

Labour Code, CQLR c C-27.

Labour Relations Act, 1995, SO 1995, c 1, Schedule A.

Labour Relations Act, RSNL 1990, c L-1.

Labour Relations Code, RSA 2000, c L-1.

Labour Relations Code, RSBC 1996, c 244.

Labour Standards Act, RSNL 1990, c L-2.

Labour Standards Act, RSNWT (Nu) 1988, c L-1.

Labour Standards Code, RSNS 1989, c 246.

Notice (Industry Canada), (2002) C Gaz I 2388 (Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council).

Official Languages Act, RSC, 1985, c 31 (4th Supp).

Personal Information Protection Act, SA 2003, c P-6.5.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSC, 1985, c P-21.

The Employment Standards Code, CCSM c E110.

The Labour Relations Act, CCSM c L10.

The Privacy Act, RSS 1978, c P-24.

The Saskatchewan Employment Act, SS 2013, c S-15.1.

Trade Union Act, RSNS 1989, c 475.

US, Bill S 3744, *Data Care Act of 2018*, 115th Cong, 2018.

US, SB 6280, *Concerning the Use of Facial Recognition Services*, 2019−2020, Reg Sess, Wash, 2020.

US, SB 5642, *New York Privacy Act*, 2019−2020, Reg Sess, NY, 2019.

Wash Const art 1.

JURISPRUDENCE

Airport Inn v Newfoundland Association of Public Employees (1992), 1992 CarswellNfld 242, [1992] Nfld LAA No 61 (Arbitrator: Alcok).

Aubry c Éditions Vice Versa Inc, [1998] 1 SCR 591, 1998 CarswellQue 4806 (SCC).

Bărbulescu v Romania, Application 61496/08, Judgment of the Court (Grand Chamber), 5 September 2017, rev'g Application 61496/08, Judgment of the Court (Fourth Section), 12 January 2016.

Dagg v Canada (Minister of Finance), [1997] 2 SCR 403, 132 FTR 55 (SCC).

Douez v Facebook Inc, 2017 SCC 33.

HJ Heinz Co of Canada Ltd v Canada (Attorney General), 2006 SCC 13.

In re Baker Hughes, Inc (Claremont, OK) and United Steelworkers International Union Region VII, Local 13-391, 128 LA (BNA) 37 (2010) (Baroni, Arb).

In re Graphic Packaging International, Inc and Graphic Communications Conference International Brotherhood of Teamsters Local 77-P, 134 LA (BNA) 369 (2014) (Wolff, Arb).

Irving Pulp & Paper Ltd. v Communications, Energy and Paperworkers Union of Canada, Local 3027, 2013 SCC 34.

Jones v Tsige, 2012 ONCA 32.

Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II")*, C-311/18, EU:C:2020:559.

Köpke v Germany, Application 420/07, Judgment of the Court (Fifth Section), 5 October 2010.

Lavigne v Canada (Commissioner of Official Languages, 2002 SCC 53.

López Ribalda and Others v Spain, Applications 1874/13 and 8567/13, Judgment of the Court (Grand Chamber), 17 October 2019, rev'g Applications 1874/13 and 8567/13, Judgment of the Court (Third Section), 9 January 2018.

Lumber & Sawmill Workers' Union, Local 2537 v KVP Co (1965), 1965 CarswellOnt 618, [1965] OLAA No 2 (Arbitrators: Wren, Robinson & Hicks).

Machtinger v HOJ Industries Ltd, [1992] 1 SCR 986, 1992 CarswellOnt 892 (SCC).

Maxam Bulk Services and International Union of Operating Engineers, Local 115 (Lebrun) (2015), 2015 CarswellBC 2277, 257 LAC (4th) 402 (Arbitrator: McConchie).

McKinley v BC Tel, 2001 SCC 38.

Millhaven Fibres Ltd, and Oil, Chemical & Atomic Workers Int'l Union, Local 9-670 (Arbitrator: Anderson), cited in *Re Lethbridge (City) and ATU, Loc 987 (Grant)* (2000), 98 LAC (4th) 264 (Arbitrator: Tettensor).

R v Jarvis, 2019 SCC 10.

R v Jones, 2017 SCC 60.

R v Spencer, 2014 SCC 43.

Re United Steelworkers of America, Local 3257 and the Steel Equipment Co Ltd (1964), 1964 CarswellOnt 498, [1964] OLAA No 5 (Arbitrators: Reville, Park & White).

Re Wasaya Airways LP and Air Line Pilots Association, International (Wyndels) (2010), 2010 CarswellNat 6233, [2010] CLAD No 297 (Arbitrator: Marcotte).

Reference Re Public Service Employee Relations Act (Alta), [1987] 1 SCR 313, 1987 CarswellAlta705 (SCC).

Steel v Coast Capital Savings Credit Union, 2015 BCCA 127, aff'g 2013 BCSC 527.

Steel v Coast Capital Savings Credit Union, 2015 BCCA 127, leave to appeal to SCC requested, 2015 CarswellBC 1979 (SCC).

Steel v Coast Capital Savings Credit Union, 2015 BCCA 127, leave to appeal to SCC refused, 2015 CarswellBC 2649 (SCC), [2015] SCCA No 217 (SCC).

The Toronto Transit Commission and The Amalgamated Transit Union, Local 113 (2019), 2019 CarswellOnt 3593, 301 LAC (4th) 1 (Arbitrator: Johnston).

UFCW, Local 401 v Alberta (Information and Privacy Commissioner), 2013 SCC 62.

United Steelworkers, Local 5795 and Iron Ore Company of Canada (2015), 2015 CarswellNfld 343, 124 CLAS 184 (Arbitrator: Oakley).

Wallace v United Grain Growers Ltd, [1997] 3 SCR 701, 1997 CarswellMan 455 (SCC).

William Scott & Co and Canadian Food and Allied Workers Union, Local P-162(1976), 1976 CarswellBC 518, [1976] 2 WLAC 585 (Arbitrators: Macdonald, Alcott & Weiler).

SECONDARY MATERIAL: MONOGRAPHS

Allen, Anita, *Uneasy Access: Privacy for Women in a Free Society* (New Jersey: Rowman & Littlefield, 1988).

Banakar, Reza, *Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity* (Lund, Sweden: Springer, 2015), online: *Springer* <www.springer.com>, DOI: <10.1007/978-3-319-09650-6>.

Bennett, Colin J, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008).

Bennett, Colin J et al, *Transparent Lives: Surveillance in Canada* (Edmonton: AU Press, Athabasca University, 2014).

Bowles, Cennydd, *Future Ethics* (United Kingdom, NowNext Press, 2018).

Brown, Douglas, Herman Bakvis & Gerald Baier, *Contested Federalism: Certainty and Ambiguity in the Canadian Federation*, 2nd ed (Oxford: Oxford University Press, 2019).

Bueckert, Melanie R, *The Law of Employee Monitoring in Canada* (Markham: LexisNexis Canada Inc, 2009).

Bloustein, Edward J, *Individual & Group Privacy* (London: Transaction Publishers, 2003).

Brunton, Finn & Helen Nissenbaum, *Obfuscation: A Users Guide for Privacy and Protest* (Cambridge, MIT Press, 2015).

Bykvist, Krister, *Utilitarianism: A Guide for the Perplexed* (London: Continuum International Publishing Group, 2010).

Cooley, Thomas M, *A Treatise on the Law of Torts on the Wrongs which arise Independent of Contract*, 2nd ed (Chicago: Callaghan and Company, 1888).

Doorey, David J, *The LAW of Work: Common Law and the Regulation of Work* (Toronto: Emond Montgomery Publications Limited, 2016).

——, *The LAW of Work: Industrial Relations and Collective Bargaining* (Toronto: Emond Montgomery Publications Limited, 2017).

DeCew, Judith Wagner, *In Pursuit of Privacy, Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997).

Dyer-Witheford, Nick, *Cyber-Proletariat: Global Labour in the Digital Vortex* (Toronto: Between the Lines, 2015).

Eggleston, Ben & Dale E Miller, *The Cambridge Companion to Utilitarianism* (Cambridge: Cambridge University press, 2014).

Eyal, Nir, with Ryan Hoover, *Hooked* (New York: Portfolio/Penguin, 2014).

Foucault, Michel, *Discipline & Punish: The Birth of the Prison*, 2nd ed, translated by Alan Sheridan (New York: Vintage Books, 1995).

——, *Power/Knowledge: Selected Interviews & Other Writings 1972–1977*, edited by Colin Gordon, translated by Colin Gordon et al (New York: Vintage Books, 1980).

——, *Surveiller et Punir: Naissance de la Prison* (Paris: Gallimard, 1975).

Gandy, Jr, Oscar H, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage* (Surrey: Ashgate, 2009).

——, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, Co: Westview Press, 1993).

Grant, Adam M, *Originals: How Non-Conformists Move the World* (New York: Viking, 2016).

Greenwald, Glenn, *No Place to Hide* (Toronto: Signal, 2014).

Harcourt, Bernard E, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015).

Harris, J W, *Legal Philosophies* (London: Butterworths & Co (Publishers) Ltd, 1980).

Hicks, Donna, *Leading with Dignity: How to Create a Culture that Brings out the Best in People* (Michigan: Yale University Press, 2018).

Hobbes, Thomas, *Leviathan*, ed by C B MacPherson (London: Penguin Looks Ltd, 1985).

Kant, Immanuel, *Critique of Pure Reason*, translated by Marcus Weigelt (London: Penguin Books Ltd, 2007).

Kateb, George, *Human Dignity* (Cambridge: Harvard University Press, 2011).

Kenny, Anthony, *A New History of Western Philosophy* (Oxford: Oxford University Press, 2012).

Kivisto, Peter, *Social Theory: Roots & Branches*, 5th ed (Oxford: Oxford University Press, 2013).

Laustsen, Carsten Bagge et al, *Social Theory: A Textbook* (London: Routledge, 2017), online: *Routledge* <https://www-taylorfrancis-com>, DOI: <10.4324/9781315657998>.

Lyon, David, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007).

——, *The Culture of Surveillance* (Cambridge: Polity Press, 2018).

MacKinnon, Catherine A, *Toward a Feminist Theory of the State* (Cambridge: Harvard University Press, 1989).

McNamee, Roger, *Zucked* (New York: Penguin Press, 2019).

McStay, Andrew, *Privacy and Philosophy* (New York: Peter Lang Publishing Inc, 2014).

Mill, John Stuart, *The Basic Writings of John Stuart Mill*, ed by Dale E Miller (New York: The Modern Library, 2002).

Mills, Jon L, *Privacy: The Lost Right* (Oxford: Oxford University press, 2008).

Mitchnick, Morton & Brian Etherington, *Labour Arbitration in Canada*, 3rd ed (Toronto: Lancaster House, 2018).

Narveson, Jan, *Morality and Utility* (Baltimore: The Johns Hopkins Press, 1967).

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010).

Orwell, George, *Nineteen Eighty-Four* (London: Penguin Books Ltd, 1990).

Otto, Marta, *The Right to Privacy in Employment: A Comparative Analysis* (Oxford: Hart Publishing, 2016).

Power, Michael E, *The Law of Privacy* (Markham: LexisNexis Canada Inc, 2013).

Prosser, William L, *Handbook of The Law of Torts,* 2nd ed (St Paul Minnesota: West Publishing Co, 1955).

Quan-Haase, Anabel, *Technology & Society Social Networks, Power, and Inequality* (Oxford: Oxford University Press, 2016).

Regan, Priscilla M, *Legislating Privacy* (North Carolina: The University of North Carolina Press, 1995).

Rengel, Alexandra, *Privacy in the 21st Century* (Netherlands: Koninklijke Brill, 2013).

Rule, James B, *Private Lives and Public Surveillance* (London: Penguin Books, 1973).

Semple, Janet, *Bentham's Prison: A Study of the Panopticon Penitentiary* (Oxford: Oxford University Press, 1993).

Smith, Brad & Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press, 2019).

Snowden, Edward, *Permanent Record* (New York: Metropolitan Books, 2019).

Solove, Daniel J, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

Sullivan, Ruth, *Sullivan on the Construction of Statutes*, 5th ed (Markham, Ontario: LexisNexis Canada Inc, 2008).

The Honourable Mr Justice Randall Scott Echlin & Christine M Thomlinson, *For Better or Worse: A Practical Guide to Canadian Employment Law*, 2nd ed (Aurora, Ontario: Canada Law Book, 2003).

Wacks, Raymond, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989).

——, *Philosophy of Law: A Very Short Introduction* (Oxford: Oxford University press, 2014).

Waldman, Ari Ezra, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018).

Westin, Alan F, *Privacy and Freedom* (New York: Atheneum, 1968).

Zuboff, Shoshana, *In the Age of the Smart Machine: The Future of Work and Power* (New York: Basic Books, 1988).

——, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019).

SECONDARY MATERIAL: JOURNAL ARTICLES AND BOOK CHAPTERS

Andrejevic, Mark, "Automating Surveillance" (2019) 17:1/2 Surveillance & Society 7, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>.

——, "Surveillance in the Big Data Era" in Kenneth D Pimple, ed, *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards* (New York: Springer, 2014) 55.

——, “The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure” (2002) 19:2 Critical Studies in Media Communication 230, online (pdf): *tandfonline* <https://www.tandfonline.com> DOI: 10.1080/07393180216561.

Anenson, T Leigh, “Announcing the Clean Hands Doctrine” (2018) 51:5 UC Davis L Rev 1827.

——, “Beyond Chafee: A Process-Based Theory of Unclean Hands” (2010) 47:3 Am Bus LJ 509.

Ball, Kirstie, “Workplace Surveillance: An Overview” (2010) 51:1 Labor History 87, online (pdf): *tandfonline* <www.tandfonline.com> DOI: <10.1080/00236561003654776>.

Ball, Kirstie S & Stephen T Margulis, “Electronic Monitoring and Surveillance in Call Centers: A Framework for Investigation” (2011) 26:2 New Technology, Work and Employment 113, online (pdf): *Wiley Online Library* <https://onlinelibrary.wiley.com/journal/1468005X>.

Ball, Kirstie, Elizabeth M Daniel & Chris Stride, “Dimensions of Employee Privacy: An Empirical Study” (2012) 25:4 Information Technology & People 376, online (pdf): *Emerald Group Publishing* <www.emeraldinsight.com> DOI: <10.1108/09593841211278785>.

Barnes, Susan B, “A Privacy Paradox: Social Networking in the United States” (2006) 11:9 First Monday, online: *First Monday* <https://firstmonday.org> DOI: 10.5210/fm.v11i9.1394.

Bennett, Collin J, “In Defence of Privacy: The Concept and the Regime” (2011) 8:4 Surveillance & Society 485, online (pdf): *Surveillance & Society* <http://www.surveillance-and-society.org>.

Blanchette, Jean-François & Deborah G Johnson, “Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness” (2002) 18:1 The Information Society 33, online (pdf): *Taylor & Francis* <www.tandfonline.com> DOI: <10.1080/01972240252818216>.

Cohen, Julie E, “What Privacy is For” (2013), 126:7 Harvard Law Review 1904.

——, “Turning Privacy Inside Out” (2019) 20.1:1 Theor Inq L, online (pdf): *ProQuest* <https://search-proquest-com> DOI: <10.1515/til-2019-0002>.

Cohen, Nicole S, “The Valorization of Surveillance: Towards a Political Economy of Facebook” in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 298.

Cownie, Fiona & Anthony Bradney, “Socio-Legal Studies” in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 40.

DeCew, Judith Wagner, “Privacy” in Andrei Marmor, ed, *The Routledge Companion to Philosophy of Law* (New York: Routledge, 2012).

Dent, Chris, “A Law Student-Oriented Taxonomy for Research in Law” (2017) 48 VUWLR 371.

Clarke, Roger & Graham Greenleaf, “Dataveillance Regulation: A Research Framework” (2017) 25:1 J L Info & Sci 104.

Foster, Lorne, Lesley Jacobs & Dr Bobby Siu, “The Ottawa Traffic Stop Race Data Collection Project” in Ontario Human Rights Commission, ed, “Racial Profiling and Human Rights”, *Canadian Diversity* 14:1 (2017) 50 online (pdf): *Ontario Human Rights Commission* <http://www.ohrc.on.ca/sites/default/files/Racial%20Profiling%20and%20Human%20Rights_Canadian%20Diversity.pdf>.

Fuchs, Christian, “Political Economy and Surveillance Theory” (2012) 39:5 Crit Sociology 671, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1177/0896920511435710>.

——, “Web 2.0, Prosumption, and Surveillance” in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 276.

Ganascia, Jean-Gabriel, “The Generalized Sousveillance Society” (2010) 49:3 Social Science Information 449, online (pdf): *SAGE Publishing* <www.sagepub.co.uk> DOI: <10.1177/0539018410371027>.

Gavison, Ruth, “Privacy and the Limits of the Law” in David Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 346.

Griffin, James, “The Human Right to Privacy” (2007) 44 San Diego L Rev 697.

Hage, Jaap, “Comparative Law as Method and the Method of Comparative Law” in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 37.

Healy, Paul & George Serafeim, “How to Scandal-Proof Your Company: A Rigorous Compliance System is Not Enough” *Harvard Business Review* (July–August 2019), 42.

Holland, Peter Jeffrey, Brian Cooper & Rob Hecker, “Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type” (2014) 44:1 Personnel Review 161, online (pdf): *Emerald Insight* <www.emeraldinsight.com> DOI: <10.1108/PR-11-2013-0211>.

Hollander, David A, “Interdisciplinary Legal Scholarship: What Can We Learn from Princeton’s Long-Standing Tradition?” (2007) 99 Law Libr J 771.

Hutchinson, Terry, “Doctrinal Research” in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 8.

Hunt, Chris D L, “Conceptualizing Privacy and Elucidating Its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort” (2001) 37 Queen's LJ 167.

Kilcommins, Shane, “Doctrinal Legal Method (Black-Letterism): Assumptions, Commitments and Shortcomings” in Laura Cahillane & Jennifer Schweppe, eds, *Legal Research Methods: Principles and Practicalities* (Dublin: Clarus Press Ltd, 2016) 7.

MacDonnell, Vanessa, “A Theory of Quasi-Constitutional Legislation” (2016) 53 Osgoode Hall LJ 508.

Mann, Steve, Jason Nolan & Barry Wellman, "Sousveillance: Inventing and Using Wearable computing Devices for Data Collection in Surveillance Environments" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 347.

Marx, Gary T, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance" (2003) 59:2 Journal of Social Issues 369, online (pdf): *The Society for the Psychological Study of Social Issues* <https://spssi-onlinelibrary-wiley-com> DOI: <10.1111/1540-4560.00069>.

Mason, Corinne & Shoshana Magnet, "Surveillance Studies and Violence Against Women" (2012) 10:2 Surveillance & Society 105, online (pdf): *Surveillance & Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>.

Miller, Paul B, "Justifying Fiduciary Duties" (2013) 58 McGill LJ 969.

Monahan, Torin, "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance" (2015) 12:2 Communication and Critical/Cultural Studies 159, online: *Taylor & Francis* <www.tandfonline.com> DOI: <10.1080/14791420.2015.1006646>.

Monahan, Torin & David Murakami Wood, "Introduction: Surveillance Studies as a Transdisciplinary Endeavor" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) ix.

——, "Society and Subjectivity" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 31.

——, "Privacy and Autonomy" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 209.

——, "Political Economy" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 281.

——, "Resistance and Opposition" in Torin Monahan & David Murakami Wood, eds, *Surveillance Studies: A Reader* (Oxford: Oxford University Press, 2018) 331.

O'Donovan, Darren, "Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls" in Laura Cahillane & Jennifer Schweppe, eds, *Legal Research Methods: Principles and Practicalities* (Dublin: Clarus Press Ltd, 2016) 107.

Pateman, Carole, "Feminist Critiques of the Public/Private Dichotomy" in Susan Moller Okin & Jane Mansbridge, eds, *Feminism* (Cambridge: Edward Elgar Publishing Company, 1994) vol 1.

Parent, W A, "A New Definition of Privacy for the Law" (1983) 2 Law and Philosophy 305.

Peikoff, Amy L, "Beyond Reductionism: Reconsidering the Right to Privacy" (2008) 3 NYU J L & Liberty 1.

——, "The Right to Privacy: Contemporary Reductionists and Their Critics" (2006) 13 Va J Soc Pol'y & L 474.

Porup, JM, "Racial Profiling in the Information Age" in Ontario Human Rights Commission, ed, "Racial Profiling and Human Rights", *Canadian Diversity* 14:1 (2017) 37 online (pdf): *Ontario Human Rights Commission* <http://www.ohrc.on.ca/sites/default/files/Racial%20Profiling%20and%20Human%20Rights_Canadian%20Diversity.pdf>.

Posner, Richard A, "The Right of Privacy" (1977-1978) 12 Ga L Rev 393.

Rule, James B, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" (2004) 54 U Toronto L J 183.

Samuel, Geoffrey, "Comparative Law and its Methodology" in Dawn Watkins & Mandy Burton, eds, *Research Methods in Law*, 2nd ed (London: Routledge, 2018) 121.

Scassa, Teresa, "Moving on from the Ombuds Model for Data Protection in Canada" (2019) 17 CJLT 90.

Sewell, Graham, James R Barker & Daniel Nyberg, "Working under Intensive Surveillance: When Does 'Measuring Everything That Moves' Become Intolerable?" (2011) 65:2 Human Relations 189, online (pdf): *SAGE Journals* <hum.sagepub.com> DOI: <10.1177/0018726711428958>.

Siems, Mathias M, "The Curious Case of Overfitting Legal Transplants" in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 133.

Smith, Gavin JD, "Surveillance, Data and Embodiment: On the Work of Being Watched" (2016) 22:2 Body & Society 108, online (pdf): *SAGE Publishing* <bod.sagepub.com> DOI: <10.1177/1357034X15623622>.

Solove, Daniel J, "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477.

Thomson, Judith Jarvis, "The Right to Privacy" (1975) 4:4 Philosophy and Public Affairs 295.

Valcke, Catherine & Mathew Grellette, "Three Functions of Function in Comparative Legal Studies" in Maurice Adams & Dirk Heirbaut, eds, *The Method and Culture of Comparative Law* (Oxford: Hart Publishing, 2015) 99.

Valentine, Sarah, "Legal Research as a Fundamental Skill: A Lifeboat for Students and Law Schools" (2010) 39 Baltimore L Rev 173.

Valsan, Remus, "Fiduciary Duties, Conflict of Interest, and Proper Exercise of Judgment" (2016) 62:1 McGill LJ 3.

Van Hoecke, Mark, "Methodology of Comparative Legal Research", Law & Method (December 2015) 1, online: *Law and Method* <http://www.lawandmethod> DOI: <10.5553/REM/.000010>.

Warren, Samuel D & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.

White, Mary Jo, "What I've Learned about White-Collar Crime" *Harvard Business Review* (July–August 2019), 58.

Young, Alyson Leigh & Anabel Quan-Haase, “Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited” (2013) 16:4 Information, Communication & Society 479, online (pdf): Taylor & Francis <www-tandfonline-com> DOI: 10.1080/1369118X.2013.777757.

Zuboff, Shoshana, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization” (2015) 30 Journal of Information Technology 75, online (pdf): *SAGE Journals* <journals.sagepub.com> DOI: <10.1057/jit.2015.5>.

SECONDARY MATERIAL: OTHER

Allen, Kate, “Toronto Police Chief Halts Use of Controversial Facial Recognition Tool” (13 February 2020), online: *The Star* <https://www.thestar.com/news/gta/2020/02/13/toronto-police-used-clearview-ai-an-incredibly-controversial-facial-recognition-tool.html>.

Amnesty International, “Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights” (21 November 2019), online (pdf): *Amnesty International* <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>.

Appleton, Lysa, “Flex Work and Telecommuting” (2018), online: *Career Professionals of Canada* <https://careerprocanada.ca/flex-work-telecommuting/>.

Article 29 Data Protection Working Party, “Guidelines on Consent under Regulation 2016/679, WP 259” (28 November 2017), online (pdf): *European Commission* <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>.

——, “Opinion 2/2017 on the Data Processing at Work, WP 249” (8 June 2017), online (pdf): *European Commission* <https://ec.europa.eu>.

——, “Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance, WP 48” (11 February 2004), online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf>.

——, "Opinion 8/2001 on the Processing of Personal Data in the Employment Context, WP 48" (13 September 2001), online (pdf): *European Commission* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf>.

Banks, Timothy, "Should PIPEDA be amended to meet GDPR requirements?" (4 April 2017), online: *iapp.org* <https://iapp.org/news/a/should-pipeda-be-amended-to-meet-gdpr-requirements/>.

Battams, Nathan, "Out of the office: workshifting and remote work in Canada" (August 2013), online (pdf): *The Vanier Institute: Fascinating Families* <http://vanierinstitute.ca/wp-content/uploads/2015/11/FFAM_2013-08-00_Workshifting-and-remote-work-Canada.pdf>.

Bimbenet, Charles, ed, *Collins LeRobert French Dictionary*, 10th ed (Glasgow: HarperCollins Publishers, 2016).

Braga, Matthew, "What happens when a Canadian border agent asks to search your phone?" (3 March 2017), online: *CBC* <https://www.cbc.ca/news/technology/border-phone-laptop-search-cbsa-canada-cbp-us-1.4002609>.

Brookes, Ian et al, eds, *Collins English Dictionary*, 13th ed (Glasgow: HarperCollins Publishers, 2018).

Brown, Donald J M, QC & David Beatty, *Canadian Labour Arbitration*, 4th ed, vol 1 (Toronto: Thomson Reuters Canada Limited, 2017).

Canada Standards Association, "CSA Standard CAN/CSA-Q830, Model Code for the Protection of Personal Information" (March 1996), online (pdf): *Canada Standards Association* <https://simson.net/ref/1996/CSA_Privacy_Standard_CSA-Q830-96.pdf>.

Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles" (January 2011), online (pdf): *Office of the Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

Cecco, Leyland, "Google Affiliate Sidewalk Labs Abruptly Abandons Toronto Smart City Project" (7 May 2020), online: *The Guardian* <https://www.theguardian.com/technology/2020/may/07/google-sidewalk-labs-toronto-smart-city-abandoned>.

City Arts & Lectures, "City Arts & Lectures presents Your Undivided Attention: Persuasive Technology: Tristan Harris in conversation with Jacob Ward" (30 April 2020), online (video): *YouTube* <https://www.youtube.com/watch?v=0TZKOuQLMfM>.

CNN Business, "Microsoft President: There is a privacy crisis" (11 October, 2019) online (video): *CNN Business* <https://www.cnn.com/videos/business/2019/10/11/brad-smith-microsoft-privacy-laws-boss-files-orig.cnn-business/video/playlists/business-boss-files/>.

Congress.Gov, "S. 3744 Data Care Act of 2018" (2020) online: *Congress.Gov* <https://www.congress.gov/bill/115th-congress/senate-bill/3744/committees>.

Cope et al, Sophia, "Digital Privacy at the U.S. Border: Protecting the Data on Your Devices" (December 2017), online (pdf): *Electronic Frontier Foundation* <https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf>.

DeCew, Judith, "Privacy" (18 January 2018), online: *Stanford Encyclopedia of Philosophy* <https://plato.stanford.edu/entries/privacy/>.

Denham, Elizabeth, "The Employment Relationship as the Privacy Laboratory" (22 November 2013), online: *Office of the Information and Privacy Commissioner for British Columbia* <https://www.oipc.bc.ca/speeches/1584>.

Dixon, Pam, "A Brief Introduction to Fair Information Practices" (5 June 2006), online: *World Privacy Forum* <https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>.

Elkouri & Elkouri, *How Arbitration Works*, 8th ed, Bloomberg BNA, (Chicago: American Bar Association, 2017) (BNA).

European Commission, "Article 29 working party archives 1997–2016" (2020), online: *European Commission* <https://ec.europa.eu/justice/article-29/documentation/index_en.htm>.

Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (24 July 2019), online: *Federal Trade Commission* <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

Geist, Michael, "PIPEDA at 20: Time for PIPEDA 2.0" (13 July 2018), online (blog): *Michael Geist* <http://www.michaelgeist.ca/2018/07/pipeda-at-20-time-for-pipeda-2-0/>.

——, "The LawBytes Podcast, Episode 2: "It's Time to Modernize the Laws"" (11 March 2019), online (podcast): *Michael Geist* <http://www.michaelgeist.ca/2019/03/the-lawbytes-podcast-episode-2-its-time-to-modernize-the-laws/>.

Gillis, Wendy & Kate Allen, "Peel and Halton Police Reveal They Too Used Controversial Facial Recognition Tool" (14 February 2020), online: *The Star* <https://www.thestar.com/news/gta/2020/02/14/peel-and-halton-police-reveal-they-too-used-controversial-facial-recognition-tool.html>.

Government of Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians" (21 May 2019), online: *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html>.

——, "Canada's Digital Charter: Trust in a Digital World" (21 May 2019), online: *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.

——, "Canada's Digital Charter: Trust in a Digital World" (21 May 2019), online (video): *Government of Canada* <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.

——, "Departments and agencies" (31 July 2017) online: *Government of Canada* <https://www.canada.ca/en/government/dept.html>.

——, "Disconnecting From Work-Related E-Communications Outside of Work Hours: Issue Paper" (4 April 2019), online: *Government of Canada* <https://www.canada.ca/en/employment-social-development/services/labour-standards/reports/disconnecting-e-communications.html>.

——, "The Constitutional Distribution of Legislative Powers" (25 July 2018), online: *Government of Canada* <https://www.canada.ca/en/intergovernmental-affairs/services/federation/distribution-legislative-powers.html>.

Government of Ontario, "Provincial ministries and agencies" (2017) online: *Government of Ontario* <https://www.ontario.ca/data/provincial-ministries-and-agencies>.

Harris, Tristan, Tim Wu & Aza Raskin, "Episode 16: When Attention Went on Sale" (28 April 2020), online (podcast): *Center for Humane Technology: Your Undivided Attention* <https://humanetech.com/>.

Harvard Business Review, "We Were Coming Up Against Everything from Organized Crime to Angry Employees" *Harvard Business Review* (July–August 2019), 54.

Herrle, Jeanette & Jesse Hirsh, "The Peril and Potential of the GDPR" (9 July 2019), online: *CIGI* <https://www.cigionline.org/articles/peril-and-potential-gdpr>.

Information Commissioner's Office, "Elizabeth Denham CBE, Information Commissioner" (2019), online: *Information Commissioner's Office* <https://ico.org.uk/about-the-ico/who-we-are/information-commissioner/>.

——, "GDPR recitals and articles" (2016), online: *Information Commissioner's Office* <https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf>.

International Association of Privacy Professionals, "Michael Geist Calls for More Robust Privacy Law at the IAPP Canadian Privacy Symposium, 2018" (13 July 2018), online (video): *YouTube* <https://www.youtube.com/watch?v=l-iIuoNqFO8>.

Kouchaki, Maryam & Isaac H Smith, "Building an Ethical Career: A Three-Stage Approach to Navigating Moral Challenges at Work" *Harvard Business Review* (January−February 2020), 135.

Lapowsky, Issie, "New York's Privacy Bill Is Even Bolder Than California's" (4 June 2019), online: *Wired* <https://www.wired.com/story/new-york-privacy-act-bolder/>.

Leblanc, Daniel, "Privacy Watchdog Takes Facebook to Court Over Possible Misuse of Personal Information" (February 2020), online: *The Globe and Mail* <https://www.theglobeandmail.com/politics/article-privacy-watchdog-takes-facebook-to-court-over-possible-misuse-of/>.

Lecturer, Grocyn, & James Morwood, eds, *Oxford Latin Desk Dictionary* (Oxford: Oxford University Press, 2005).

Lynch, Jennifer, "Face Off: Law Enforcement Use of Face Recognition Technology" (May 2019), online (pdf): *Electronic Frontier Foundation* <https://www.eff.org/files/2019/05/28/face-off-report.pdf>.

Montpetit, Jonathan, "Personal Data of 2.7 Million People Leaked from Desjardins" (20 June 2019), online: *CBC News Montreal* <https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297>.

Morissette, René, "Changing Characteristics of Canadian Jobs, 1981 to 2018" (30 November 2018) at 1, online (pdf): *Statistics Canada: Economic Insights* <https://www150.statcan.gc.ca/n1/en/pub/11-626-x/11-626-x2018086-eng.pdf?st=GTmudv2A>.

New York State Senate, "Senate Bill S5642" (2020) online: *New York State Senate* <https://www.nysenate.gov/legislation/bills/2019/s5642>.

OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980), online: *OECD* <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

OECD, "The OECD Privacy Framework" (2013), online (pdf): *OECD* <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

Office of the Prime Minister, "Minister of Innovation, Science and Industry Mandate Letter" (December, 2019), online: *Prime Minster of Canada* <https://pm.gc.ca/en/mandate-letters/minister-innovation-science-and-industry-mandate-letter>.

Office of the Privacy Commissioner of Canada, "10 Workplace Tips for Protecting Personal Information on Mobile Devices" (January 2011), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_46_dpd/>.

——, "2018-2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act"*(10 December 2019), online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf>.

——, "A Full Year of Mandatory Data Breach Reporting: What We've Learned and What Businesses Need to Know" (31 October 2019), online (blog): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/blog/20191031/>.

——, "Appearance Before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)" (16 February 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20170216/>.

——, "Canada's Access to Information and Privacy Guardians Urge Governments to Modernize Legislation to Better Protect Canadians" (6 November 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/>.

——, "Commissioners Launch Joint Investigation into Clearview AI Amid Growing Concerns Over Use of Facial Recognition Technology" (21 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/>.

——, "Contemplating a Bring Your Own Device (BYOD) program?" (August 2015), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/tips_byod/>.

——, "Guidance on Covert Video Surveillance in the Private Sector" (May 2009), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/>.

——, “Guidance on Overt Video Surveillance in the Private Sector” (March 2008), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gl_vs_080306/>.

——, “Guidelines for Obtaining Meaningful Consent” (24 May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

——, “Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?” (22 July 2015), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/>.

——, “Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia” (25 April, 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.

——, “Notice of Application with the Federal Court Against Facebook, Inc” (6 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/court_p/na_fb_20200206/>.

——, “OPC Launches Investigation into Capital One Breach” (31 July 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190731_02/>.

——, “OPC Launches Investigation into RCMP’s Use of Facial Recognition Technology” (28 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/>.

——, “PIPEDA Fair Information Principles” (May 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>.

——, “PIPEDA in Brief” (May 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>.

——, “Privacy and Social Media in the Workplace” (August 2019), online: *Office of the Privacy Commissioner of Canada* <https://priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/02_05_d_41_sn/>.

——, “Privacy Commissioner Denounces Slow Progress on Fixing Outdated Privacy Laws” (27 September 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180927/>.

——, “Privacy Commissioner Files Notice of Application with the Federal Court Against Facebook, Inc” (6 February 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206/>.

——, “Provincial Legislation Deemed Substantially Similar to PIPEDA” (29 May 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/>.

——, “Quebec, Federal Privacy Commissioners Investigate Desjardins Breach” (8 July 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190708/>.

——, “Questions and Answers Regarding the Application of *PIPEDA*, Alberta and British Columbia's *Personal Information Protection Acts*” (November 2004), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/>.

——, “Remarks by Privacy Commissioner of Canada regarding his 2018-19 Annual Report to Parliament” (10 December 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20191210/>.

——, “Remarks by Privacy Commissioner of Canada Regarding the Facebook/Cambridge-Analytica investigation” (25 April 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20190425/>.

——, “Report to Parliament Concerning Substantially Similar Provincial Legislation” (June 2003), online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/2360/leg-rp_030611_e.pdf>.

——, “Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners” (1−2 October 2019), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191106/>.

——, “The Privacy Commissioner of Canada” (14 December 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/who-we-are/the-privacy-commissioner-of-canada/>.

Ontario Human Rights Commission, “Racial Profiling and Human Rights”, *Canadian Diversity* 14:1 (2017) 1 online (pdf): *Ontario Human Rights Commission* <http://www.ohrc.on.ca/sites/default/files/Racial%20Profiling%20and%20Human%20Rights_Canadian%20Diversity.pdf>.

——, “Racial Profiling Doesn’t Work” (2020), online: *Ontario Human Rights Commission* <http://www.ohrc.on.ca/en/paying-price-human-cost-racial-profiling/racial-profiling-doesnt-work>.

Parliament of Canada, “S-21, An Act to Guarantee the Human Right to Privacy” (2001–2002), online: *Parliament of Canada* <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=4772262&View=0>.

Privacy by Design Centre of Excellence, “Dr. Ann Cavoukian, Distinguished Expert-in-Residence” (2020), online: *Ryerson University* <https://www.ryerson.ca/pbdce/about/ann-cavoukian/>.

Russell, Andrew, “RCMP Used Clearview AI Facial Recognition Tool in 15 Child Exploitation Cases, Helped Rescue 2 Kids” (27 February 2020), online: *Global News* <https://globalnews.ca/news/6605675/rcmp-used-clearview-ai-child-exploitation/>.

Smith, Buckley, “Laying Blame on Employee in Desjardins Data Breach is Ignoring the Big Picture, Security Experts Say” (21 June 2019), online: *ITWorldCanada* <https://www.itworldcanada.com/article/laying-blame-on-employee-in-desjardins-data-breach-is-ignoring-the-big-picture-security-experts-says/419299>.

Stanley, Jay, “The Dawn of Robot Surveillance, AI, Video Analytics, and Privacy” (2019), online (pdf): *American Civil Liberties Union* <https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf>.

Statistics Canada, “Impact of Cybercrime on Canadian Businesses, 2017” (15 October 2018), online (pdf): *Statistics Canada: The Daily* <https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm>.

Stenson, Angus ed, *Oxford Dictionary of English*, 3rd ed (Oxford: Oxford University Press, 2010).

Stoddart, Jennifer, “Annual Reports to Parliament 2004 on the Personal Information Protection and Electronic Documents Act” (October 2005), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/200405/2004_pipeda/>.

The Standing Senate Committee on Social Affairs, Science and Technology, “Report of the Committee” (14 December 2001), online: *Senate of Canada* <https://sencanada.ca/Content/SEN/Committee/371/soci/rep/rep13dec01-e.htm>.

Suarez, Juan-Louis, “Sidewalk Labs Dumping the Quayside Development Might Signal a Bright Future for Toronto” (15 May 2020), online: *The Star* <https://www.thestar.com/opinion/contributors/2020/05/15/sidewalk-labs-dumping-the-quayside-development-might-signal-a-bright-future-for-toronto.html>.

Tunney, Catherine, “Privacy Watchdog Taking Facebook to Court, Says Company Breached Privacy Laws” (25 April 2019), online: *CBC News* <https://www.cbc.ca/news/politics/privacy-watchdog-cambridge-analytica-facebook-1.5110304>.

——, “RCMP’s Use of Clearview AI Facial Recognition Technology Under Investigation” (28 February 2020), online: *CBC News* <https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479673>.

Washington State Legislature, “Bill Information: SB 6280” (12 April 2020), online: *Washington State Legislature* <https://app.leg.wa.gov/billsummary?BillNumber=6280&Initiative=false&Year=2019>.

Zimmer, Bob, “Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics (February 2018), online (pdf): *House of Commons* <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf >.

Zimonjic, Peter, “Proceedings Launched After Facebook Refused to Implement Commissioner's Recommendations to Protect Privacy” (6 February 2020), online: *CBC News* <https://www.cbc.ca/news/politics/facebook-privacy-commissioner-hearing-1.5454525>.

Appendices

Appendix A: Privacy Provisions Analyzed in Chapter 4, Theme 1

Canada

Section 3 of *PIPEDA:*[1766]

> Purpose
>
> 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[1767]

Principles 2 and 4 in Clauses 4.2 and 4.4 of Schedule 1 of *PIPEDA*:[1768]

> 4.2 Principle 2 — Identifying Purposes
>
> The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
>
> 4.2.1
>
> The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).
>
> 4.2.2
>
> Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

[1766] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 at s 3 [*PIPEDA*].
[1767] *Ibid.*
[1768] *Ibid* at Schedule 1, cl 4.2, 4.4.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.4 Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).[1769]

Section 5 of the *Québec Charter:*[1770]

Fundamental Freedoms and Rights

5. Every person has a right to respect for his private life.[1771]

Sections 1−5 of *Bill S-21 (Privacy Rights Charter)*:[1772]

Short title

1. This Act may be cited as the Privacy Rights Charter.

Purpose

2. The purpose of this Act is to give effect to the principles that

(a) privacy is essential to an individual's dignity, integrity, autonomy, well-being and freedom, and to the full and meaningful exercise of human rights and freedoms;

(b) there is a legal right to privacy;

(c) an infringement of the right to privacy, to be lawful, must be justifiable.

Right to privacy

3. Every individual has a right to privacy, including

(a) physical privacy;

(b) freedom from surveillance;

(c) freedom from monitoring or interception of their private communications; and

(d) freedom from the collection, use and disclosure of their personal information.

[1769] *Ibid.*
[1770] *Charter of Human Rights and Freedoms*, CQLR c C-12 at s 5 [*Québec Charter*].
[1771] *Ibid*.
[1772] Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess, 37th Parl, 2001 (first reading 13 March 2001, dropped from the Senate Order Paper in 2002) [*Bill S-21 (Privacy Rights Charter)*].

Remedy

4. (1) Every individual is entitled to claim and enforce their right to privacy and to refuse to unjustifiably infringe the right to privacy of another individual.

No reprisal

(2) No person shall take or threaten to take reprisal measures against an individual who claims or enforces their right to privacy or who refuses to unjustifiably infringe the right to privacy of another individual.

Prohibition

(3) No person shall unjustifiably infringe an individual's right to privacy.

Infringement

5. (1) A limit on or interference with an individual's privacy infringes that individual's right to privacy.

Justification

(2) An infringement of an individual's right to privacy is justifiable if the infringement is reasonable and can be demonstrably justified in a free and democratic society.

Test

(3) An infringement is justifiable if:

(a) it is lawful;

(b) it is necessary to achieve an objective that is compelled by the need to respect another individual human right or another interest in the public good and is sufficiently important to warrant infringing the right to privacy;

(c) the objective cannot be achieved by another measure that infringes privacy less; and

(d) the importance of the objective and the beneficial effects of the infringement outweigh the detrimental effects on privacy.

Consent

> (4) An interference with an individual's privacy does not infringe that individual's right to privacy if the interference is done with the free and fully informed consent of the individual.[1773]

United States

Section 1798.140(e) and (q) of the *California Consumer Privacy Act*[1774] define collection and processing:

> (e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.
>
> (q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.[1775]

Section 1102 of *Bill S5642 (New York Privacy Act):*[1776]

> § 1102. Data fiduciary. 1. Personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.
>
> (a) Every legal entity, or affiliate of such entity, and every controller and data broker to which this article applies shall:
>
> (i) reasonably secure personal data from unauthorized access; and
>
> (ii) promptly inform a consumer of any breach of the duty described in this paragraph with respect to personal data of such consumer.
>
> (b) A legal entity, an affiliate of such entity, controller or data broker may not use personal data, or data derived from personal data, in any way that:

[1773] *Ibid.*
[1774] *California Consumer Privacy Act of 2018*, 3 CIV 1.81.5 (2018) at § 1798.140(e), (q) [*California Consumer Privacy Act*].
[1775] *Ibid.*
[1776] US, SB 5642, *New York Privacy Act*, 2019−2020, Reg Sess, NY, 2019 at § 1102 [*Bill S5642 (New York Privacy Act)*].

(i) will benefit the online service provider to the detriment of an end user; and

(ii) (A) will result in reasonably foreseeable and material physical or financial harm to a consumer; or

(B) would be unexpected and highly offensive to a reasonable consumer.

(c) A legal entity, or affiliate of such entity, controller or data broker:

(i) may not disclose or sell personal data to, or share personal data with, any other person except as consistent with the duties of care and loyalty under paragraphs (a) and (b) of this subdivision;

(ii) may not disclose or sell personal data to, or share personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed under this section; and

(iii) shall take reasonable steps to ensure that the practices of any person to whom the entity, or affiliate of such entity, controller or data broker discloses or sells, or with whom the entity, or affiliate of such entity, controller or data broker shares. Personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (ii) of this paragraph, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.

2. For the purposes of this section the term "privacy risk" means potential adverse consequences to consumers and society arising from the processing of personal data, including, but not limited to:

(a) direct or indirect financial loss or economic harm;

(b) physical harm;

(c) psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(d) significant inconvenience or expenditure of time;

(e) adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(f) stigmatization or reputational harm;

(g) disruption and intrusion from unwanted commercial communications or contacts;

(h) price discrimination;

> (i) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller assessing privacy risk, that:
>
> (A) alters that individual's experiences;
>
> (B) limits that individual's choices;
>
> (C) influences that individual's responses; or
>
> (D) predetermines results; or
>
> (j) other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.
>
> 3. The fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker, to whom this article apples.[1777]

Section 1 of *Bill SB 6280 (Washington Facial Recognition)*:[1778]

> NEW SECTION. Sec. 1. The legislature finds that:
>
> (1) Unconstrained use of facial recognition services by state and local government agencies poses broad social ramifications that should be considered and addressed. Accordingly, legislation is required to establish safeguards that will allow state and local government agencies to use facial recognition services in a manner that benefits society while prohibiting uses that threaten our democratic freedoms and put our civil liberties at risk.
>
> (2) However, state and local government agencies may use facial recognition services to locate or identify missing persons, and identify deceased persons, including missing or murdered indigenous women, subjects of Amber alerts and silver alerts, and other possible crime victims, for the purposes of keeping the public safe.[1779]

Section 2(2−5), (9−12) of *Bill SB 6280 (Washington Facial Recognition)*[1780]defines enroll, facial recognition service, facial template, identification, ongoing surveillance, persistent tracking, recognition, and verification:

[1777] *Ibid.* The line numbers and underline formatting are not included in this passage.
[1778] US, SB 6280, *Concerning the Use of Facial Recognition Services*, 2019−2020, Reg Sess, Wash, 2020 at § 1[*Bill SB 6280 (Washington Facial Recognition)*]. The line numbers and underline formatting are not included in this passages with respect to this bill.
[1779] *Ibid.*
[1780] *Ibid* at § 2(1)−(5), (9−12).

NEW SECTION. Sec. 2. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(2) "Enroll," "enrolled," or "enrolling" means the process by which a facial recognition service creates a facial template from one or more images of an individual and adds the facial template to a gallery used by the facial recognition service for recognition or persistent tracking of individuals. It also includes the act of adding an existing facial template directly into a gallery used by a facial recognition service.

(3)(a) "Facial recognition service" means technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking of individuals in still or video images.

(b) "Facial recognition service" does not include: (i) The analysis of facial features to grant or deny access to an electronic device; or (ii) the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.

(4) "Facial template" means the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service.

(5) "Identification" means the use of a facial recognition service by a state or local government agency to determine whether an unknown individual matches any individual whose identity is known to the state or local government agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

(9) "Ongoing surveillance" means using a facial recognition service to track the physical movements of a specified individual through one or more public places over time, whether in real time or through application of a facial recognition service to historical records. It does not include a single recognition or attempted recognition of an individual, if no attempt is made to subsequently track that individual's movement over time after they have been recognized.

(10) "Persistent tracking" means the use of a facial recognition service by a state or local government agency to track the movements of an individual on a persistent basis without identification or verification of that individual. Such tracking becomes persistent as soon as:

(a) The facial template that permits the tracking is maintained for more than forty-eight hours after first enrolling that template; or

(b) Data created by the facial recognition service is linked to any other data such that the individual who has been tracked is identified or identifiable.

> (11) "Recognition" means the use of a facial recognition service by a state or local government agency to determine whether an unknown individual matches:
>
> (a) Any individual who has been enrolled in a gallery used by the facial recognition service; or
>
> (b) A specific individual who has been enrolled in a gallery used by the facial recognition service.
>
> (12) "Verification" means the use of a facial recognition service by a state or local government agency to determine whether an individual is a specific individual whose identity is known to the state or local government agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.[1781]

Section 3 of *Bill SB 6280 (Washington Facial Recognition)*:[1782]

> NEW SECTION. Sec. 3. (1) A state or local government agency using or intending to develop, procure, or use a facial recognition service must file with a legislative authority a notice of intent to develop, procure, or use a facial recognition service and specify a purpose for which the technology is to be used. A state or local government agency may commence the accountability report once it files the notice of intent by the legislative authority.
>
> (2) Prior to developing, procuring, or using a facial recognition service, a state or local government agency must produce an accountability report for that service. Each accountability report must include, at minimum, clear and understandable statements of the following:
>
> (a)(i) The name of the facial recognition service, vendor, and version; and (ii) a description of its general capabilities and limitations, including reasonably foreseeable capabilities outside the scope of the proposed use of the agency;
>
> (b)(i) The type or types of data inputs that the technology uses; (ii) how that data is generated, collected, and processed; and (iii) the type or types of data the system is reasonably likely to generate;
>
> (c)(i) A description of the purpose and proposed use of the facial recognition service, including what decision or decisions will be used to make or support it; (ii) whether it is a final or support decision system; and (iii) its intended benefits, including any data or research demonstrating those benefits;
>
> (d) A clear use and data management policy, including protocols for the following:

[1781] *Ibid.*
[1782] *Ibid* at § 3.

(i) How and when the facial recognition service will be deployed or used and by whom including, but not limited to, the factors that will be used to determine where, when, and how the technology is deployed, and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances. If the facial recognition service will be operated or used by another entity on the agency's behalf, the facial recognition service accountability report must explicitly include a description of the other entity's access and any applicable protocols;

(ii) Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose or purposes for which the facial recognition service will be used;

(iii) Data integrity and retention policies applicable to the data collected using the facial recognition service, including how the agency will maintain and update records used in connection with the service, how long the agency will keep the data, and the processes by which data will be deleted;

(iv) Any additional rules that will govern use of the facial recognition service and what processes will be required prior to each use of the facial recognition service;

(v) Data security measures applicable to the facial recognition service including how data collected using the facial recognition service will be securely stored and accessed, if and why an agency intends to share access to the facial recognition service or the data from that facial recognition service with any other entity, and the rules and procedures by which an agency sharing data with any other entity will ensure that such entities comply with the sharing agency's use and data management policy as part of the data sharing agreement;

(vi) How the facial recognition service provider intends to fulfill security breach notification requirements pursuant to chapter 19.255 RCW and how the agency intends to fulfill security breach notification requirements pursuant to RCW 42.56.590; and

(vii) The agency's training procedures, including those implemented in accordance with section 7 of this act, and how the agency will ensure that all personnel who operate the facial recognition service or access its data are knowledgeable about and able to ensure compliance with the use and data management policy prior to use of the facial recognition service;

(e) The agency's testing procedures, including its processes for periodically undertaking operational tests of the facial recognition service in accordance with section 5 of this act;

(f) Information on the facial recognition service's rate of false matches, potential impacts on protected subpopulations, and how the agency will address error rates, determined independently, greater than one percent;

> (g) A description of any potential impacts of the facial recognition service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the facial recognition service; and
>
> (h) The agency's procedures for receiving feedback, including the channels for receiving feedback from individuals affected by the use of the facial recognition service and from the community at large, as well as the procedures for responding to feedback.
>
> (3) Prior to finalizing the accountability report, the agency must:
>
> (a) Allow for a public review and comment period;
>
> (b) Hold at least three community consultation meetings; and
>
> (c) Consider the issues raised by the public through the public review and comment period and the community consultation meetings.
>
> (4) The final accountability report must be updated every two years and submitted to a legislative authority.
>
> (5) The final adopted accountability report must be clearly communicated to the public at least ninety days prior to the agency putting the facial recognition service into operational use, posted on the agency's public web site, and submitted to a legislative authority. The legislative authority must post each submitted accountability report on its public web site.
>
> (6) A state or local government agency seeking to procure a facial recognition service must require vendors to disclose any complaints or reports of bias regarding the service.
>
> (7) An agency seeking to use a facial recognition service for a purpose not disclosed in the agency's existing accountability report must first seek public comment and community consultation on the proposed new use and adopt an updated accountability report pursuant to the requirements contained in this section.
>
> (8) This section does not apply to a facial recognition service under contract as of the effective date of this section. An agency must fulfill the requirements of this section upon renewal or extension of the contract.[1783]

Section 8(1) of *Bill SB 6280 (Washington Facial Recognition)*:[1784]

> NEW SECTION. Sec. 8. (1) A state or local government agency must disclose their use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial.[1785]

[1783] *Ibid.*
[1784] *Ibid* at § 8(1).
[1785] *Ibid.*

Section 11 of *Bill SB 6280 (Washington Facial Recognition)*:[1786]

> NEW SECTION. Sec. 11. (1) A state or local government agency may not use a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless:
>
> (a) A warrant is obtained authorizing the use of the service for those purposes;
>
> (b) Exigent circumstances exist; or
>
> (c) A court order is obtained authorizing the use of the service for the sole purpose of locating or identifying a missing person, or identifying a deceased person. A court may issue an ex parte order under this subsection (1)(c) if a law enforcement officer certifies and the court finds that the information likely to be obtained is relevant to locating or identifying a missing person, or identifying a deceased person.
>
> (2) A state or local government agency may not apply a facial recognition service to any individual based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law. This subsection does not condone profiling including, but not limited to, predictive law enforcement tools.
>
> (3) A state or local government agency may not use a facial recognition service to create a record describing any individual's exercise of rights guaranteed by the First Amendment of the United States Constitution and by Article I, section 5 of the state Constitution.
>
> (4) A law enforcement agency that utilizes body worn camera recordings shall comply with the provisions of RCW 42.56.240(14).
>
> (5) A state or local law enforcement agency may not use the results of a facial recognition service as the sole basis to establish probable cause in a criminal investigation. The results of a facial recognition service may be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation.
>
> (6) A state or local law enforcement agency may not use a facial recognition service to identify an individual based on a sketch or other manually produced image.
>
> (7) A state or local law enforcement agency may not substantively manipulate an image for use in a facial recognition service in a manner not

[1786] *Ibid* at § 11.

> consistent with the facial recognition service provider's intended use and training.[1787]

Section 1 of Article 1 of the *California Constitution:*[1788]

> Declaration of Rights
>
> 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[1789]

European Union

Article 1(2) of the *GDPR:*[1790]

> Subject-matter and objectives
>
> 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[1791]

Article 4(2) and (4) of the *GDPR*[1792] defines processing and profiling:

> Definitions
>
> (2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
>
> (4) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[1793]

[1787] *Ibid.*
[1788] Cal Const art I at § 1 [*California Constitution*].
[1789] *Ibid*.
[1790] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L119/1 at art 1(2) [*GDPR*].
[1791] *Ibid.*
[1792] *Ibid* at art 4(2), (4).
[1793] *Ibid*.

Article 5 of the *GDPR:*[1794]

> Principles relating to processing of personal data
>
> 1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
>
> 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').[1795]

Article 9(1) of the *GDPR:*[1796]

[1794] *Ibid* at art 5.
[1795] *Ibid.*
[1796] *Ibid* at art 9(1).

> Processing of special categories of personal data
>
> 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[1797]

Article 21(1) of the *GDPR:*[1798]

> Right to object
>
> 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.[1799]

Article 22 of the *GDPR:*[1800]

> Automated individual decision-making, including profiling
>
> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
>
> 2. Paragraph 1 shall not apply if the decision:
>
> (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
>
> (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> (c) is based on the data subject's explicit consent.
>
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

[1797] *Ibid.*
[1798] *Ibid* at art 21(1).
[1799] *Ibid.*
[1800] *Ibid* at art 22.

> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.[1801]

Article 23 of the *GDPR:*[1802]

> Restrictions
>
> 1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
>
> (a) national security;
>
> (b) defence;
>
> (c) public security;
>
> (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
>
> (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
>
> (f) the protection of judicial independence and judicial proceedings;
>
> (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
>
> (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
>
> (i) the protection of the data subject or the rights and freedoms of others;
>
> (j) the enforcement of civil law claims.
>
> 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
>
> (a) the purposes of the processing or categories of processing;
>
> (b) the categories of personal data;

[1801] *Ibid*.
[1802] *Ibid* at art 23.

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.[1803]

Article 25(1) and (2) of the *GDPR:*[1804]

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[1805]

Article 35(1) and (7) of the *GDPR:*[1806]

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the

---

[1803] *Ibid.*
[1804] *Ibid* at art 25(1)−(2).
[1805] *Ibid.*
[1806] *Ibid* at art 35(1), (7).

> protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
>
> 7. The assessment shall contain at least:
>
> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[1807]

Article 8 of the *EU Convention:*[1808]

> Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[1809]

[1807] *Ibid.*
[1808] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5 (1950) at art 8 [*EU Convention*].
[1809] *Ibid*.

Appendix B: Privacy Provisions Analyzed in Chapter 4, Theme 2

Canada

In Canada, section 2(1) of *PIPEDA*[1810] defines personal information:

> 2(1) personal information means information about an identifiable individual.[1811]

Section 6.1 of *PIPEDA:*[1812]

> Valid consent
>
> 6.1 For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.[1813]

Section 7 of *PIPEDA:*[1814]

> Collection without knowledge or consent
>
> 7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if
>
> (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
>
> (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
>
> (b.1) it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim;

[1810] *PIPEDA, supra* note 1766at s 2(1).
[1811] *Ibid.*
[1812] *PIPEDA, supra* note 1766at s 6.1.
[1813] *Ibid.*
[1814] *Ibid* at s 7.

(b.2) it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced;

(c) the collection is solely for journalistic, artistic or literary purposes;

(d) the information is publicly available and is specified by the regulations; or

(e) the collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(c.1)(i) or (d)(ii), or

(ii) that is required by law.

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(b.1) the information is contained in a witness statement and the use is necessary to assess, process or settle an insurance claim;

(b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;

(c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;

(c.1) it is publicly available and is specified by the regulations; or

(d) it was collected under paragraph (1)(a), (b) or (e).

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(b) for the purpose of collecting a debt owed by the individual to the organization;

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or

(iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;

(c.2) made to the government institution mentioned in section 7 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act as required by that section;

(d) made on the initiative of the organization to a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

(d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;

(d.3) made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and

(i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,

(ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and

(iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;

(d.4) necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

(e.1) of information that is contained in a witness statement and the disclosure is necessary to assess, process or settle an insurance claim;

(e.2) of information that was produced by the individual in the course of their employment, business or profession and the disclosure is consistent with the purposes for which the information was produced;

(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(h) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(h.1) of information that is publicly available and is specified by the regulations; or

(h.2) [Repealed, 2015, c. 32, s. 6]

(i) required by law.

Use without consent

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Disclosure without consent

(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.1).[1815]

Section 7.3 of *PIPEDA*:[1816]

Employment relationship

7.3 In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if

(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and

---

[1815] *Ibid.*
[1816] *Ibid* at s 7.3.

> (b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.[1817]

Section 7.4 of *PIPEDA:*[1818]

> Use without consent
>
> 7.4 (1) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.
>
> Disclosure without consent
>
> (2) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.[1819]

Sections 10.1–10.3 of *PIPEDA:*[1820]

> Report to Commissioner
>
> 10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.
>
> Report requirements
>
> (2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.
>
> Notification to individual
>
> (3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
>
> Contents of notification

[1817] *Ibid.*
[1818] *Ibid* at s 7.4.
[1819] *Ibid*.
[1820] *Ibid* at ss 10.1–10.3.

(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.

Form and manner

(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.

Time to give notification

(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

Definition of significant harm

(7) For the purpose of this section, significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Real risk of significant harm — factors

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information involved in the breach;

(b) the probability that the personal information has been, is being or will be misused; and

(c) any other prescribed factor.[1821]

Section 27.1(1) of *PIPEDA*:[1822]

Prohibition

27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that

---

[1821] *Ibid.*
[1822] *Ibid* at s 27.1(1).

> (a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1 or 1.1;
>
> (b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1 or 1.1;
>
> (c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 or 1.1 not be contravened; or
>
> (d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).[1823]

Section 28 of *PIPEDA*:[1824]

> Offence and punishment
>
> 28 Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of
>
> (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or
>
> (b) an indictable offence and liable to a fine not exceeding $100,000.[1825]

Principle 3 under Clause 4.3 in Schedule 1 of *PIPEDA:*[1826]

> 4.3 Principle 3 – Consent
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the

---

[1823] *Ibid.*
[1824] *Ibid* at 28.
[1825] *Ibid.*
[1826] *Ibid* at Schedule 1, cl 4.3.

individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

> An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.[1827]

Section 2−6 of the *PIPEDA Breach Regulations*:[1828]

> Report to Commissioner
>
> Report — content, form and manner
>
> 2 (1) A report of a breach of security safeguards referred to in subsection 10.1(2) of the Act must be in writing and must contain
>
> (a) a description of the circumstances of the breach and, if known, the cause;
>
> (b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
>
> (c) a description of the personal information that is the subject of the breach to the extent that the information is known;
>
> (d) the number of individuals affected by the breach or, if unknown, the approximate number;
>
> (e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
>
> (f) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; and
>
> (g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.
>
> New information
>
> (2) An organization may submit to the Commissioner any new information referred to in subsection (1) that the organization becomes aware of after having made the report.
>
> Means of communication
>
> (3) The report may be sent to the Commissioner by any secure means of communication.

[1827] *Ibid.*
[1828] *Breach of Security Safeguards Regulations* (SOR/2018-64) at s 2−6 [*PIPEDA Breach Regulations*].

Notification to Affected Individual

Contents of notification

3 A notification provided by an organization, in accordance with subsection 10.1(3) of the Act, to an affected individual with respect to a breach of security safeguards must contain

(a) a description of the circumstances of the breach;

(b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

(c) a description of the personal information that is the subject of the breach to the extent that the information is known;

(d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;

(e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

(f) contact information that the affected individual can use to obtain further information about the breach.

Direct notification — form and manner

4 For the purposes of subsection 10.1(5) of the Act, direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.

Indirect notification — circumstances

5 (1) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by an organization in any of the following circumstances:

(a) direct notification would be likely to cause further harm to the affected individual;

(b) direct notification would be likely to cause undue hardship for the organization; or

(c) the organization does not have contact information for the affected individual.

Indirect notification — form and manner

> (2) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.
>
> Record-keeping
>
> Record-keeping requirements
>
> 6 (1) For the purposes of subsection 10.3(1) of the Act, an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred.
>
> Compliance
>
> (2) The record referred to in subsection 10.3(1) of the Act must contain any information that enables the Commissioner to verify compliance with subsections 10.1(1) and (3) of the Act.[1829]

In section 1 of the *BC PIPA*,[1830] defines personal information and employee personal information:

> "employee personal information" means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment;
>
> "personal information" means information about an identifiable individual and includes employee personal information but does not include
>
> (a) contact information, or
>
> (b) work product information.[1831]

Section 7 of the *BC PIPA*[1832] defines consent as:

> Provision of consent
>
> **7**(1) An individual has not given consent under this Act to an organization unless
>
> (a) the organization has provided the individual with the information required under section 10(1), and

---

[1829] *Ibid.*
[1830] *BC PIPA, supra* note 1832 at s 1.
[1831] *Ibid.*
[1832] *Personal Information Protection Act*, SBC 2003, c 63 at s 7 [*BC PIPA*].

> (b) the individual's consent is provided in accordance with this Act.
>
> (2) An organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.
>
> (3) If an organization attempts to obtain consent for collecting, using or disclosing personal information by
>
> (a) providing false or misleading information respecting the collection, use or disclosure of the information, or
>
> (b) using deceptive or misleading practices
>
> any consent provided in those circumstances is not validly given.[1833]

Section 8(3) of the *BC PIPA*:[1834]

> (3) An organization may collect, use or disclose personal information about an individual for specified purposes if
>
> (a) the organization provides the individual with a notice, in a form the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual's personal information for those purposes,
>
> (b) the organization gives the individual a reasonable opportunity to decline within a reasonable time to have his or her personal information collected, used or disclosed for those purposes,
>
> (c) the individual does not decline, within the time allowed under paragraph (b), the proposed collection, use or disclosure, and
>
> (d) the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.[1835]

Section 9(3) of the *BC PIPA*:[1836]

> (3) An organization must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal information related to the individual.[1837]

[1833] *Ibid.*
[1834] *Ibid* at s 8(3).
[1835] *Ibid.*
[1836] *Ibid* at s 9(3).

Sections 13, 16, and 19 of the *BC PIPA*:[1838]

> Collection of employee personal information
>
> 13 (1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual.
>
> (2) An organization may not collect employee personal information without the consent of the individual unless
>
> (a) section 12 allows the collection of the employee personal information without consent, or
>
> (b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.
>
> (3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the employee personal information without the consent of the individual.
>
> (4) Subsection (3) does not apply to employee personal information if section 12 allows it to be collected without the consent of the individual.
>
> Use of employee personal information
>
> 16 (1) Subject to subsection (2), an organization may use employee personal information without the consent of the individual.
>
> (2) An organization may not use employee personal information without the consent of the individual unless
>
> (a) section 15 allows the use of the employee personal information without consent, or
>
> (b) the use is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.
>
> (3) An organization must notify an individual that it will be using employee personal information about the individual and the purposes for the use

---

[1837] *Ibid.*
[1838] *Ibid* at ss 13, 16, 19.

before the organization uses the employee personal information without the consent of the individual.

(4) Subsection (3) does not apply to employee personal information if section 15 allows it to be used without the consent of the individual.

Disclosure of employee personal information

19 (1) Subject to subsection (2), an organization may disclose employee personal information without the consent of the individual.

(2) An organization may not disclose employee personal information without the consent of the individual unless

(a) section 18 allows the disclosure of the employee personal information without consent, or

(b) the disclosure is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.

(3) An organization must notify an individual that it will be disclosing employee personal information about the individual and the purposes for the disclosure before the organization discloses employee personal information about the individual without the consent of the individual.

(4) Subsection (3) does not apply to employee personal information if section 18 allows it to be disclosed without the consent of the individual.[1839]

Section 14 of the *QC Act:*[1840]

Retention, use and non-communication of information

14. Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.

Consent given otherwise than in accordance with the first paragraph is without effect.[1841]

[1839] *Ibid*.
[1840] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 at s 14 [*QC Act*].
[1841] *Ibid.*

United States

Section 980 of the *California Labor Code:*[1842]

> 980.
>
> (a) As used in this chapter, "social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.
>
> (b) An employer shall not require or request an employee or applicant for employment to do any of the following:
>
> (1) Disclose a username or password for the purpose of accessing personal social media.
>
> (2) Access personal social media in the presence of the employer.
>
> (3) Divulge any personal social media, except as provided in subdivision (c).
>
> (c) Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding.
>
> (d) Nothing in this section precludes an employer from requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device.
>
> (e) An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section. However, this section does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law.[1843]

Section 1798.120(a) and (b)[1844] of the *California Consumer Privacy Act:*

> 1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties

---

[1842] Cal Lab Code (2012) at § 980 [*California Labor Code*].
[1843] *Ibid.*
[1844] *California Consumer Privacy Act*, *supra* note 1774 at § 1798.120(a)−(b).

not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.[1845]

Section 1798.125(a)(1) of the *California Consumer Privacy Act*:[1846]

1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.[1847]

Section 1798.145(a)(1) to (5) of the *California Consumer Privacy Act*:[1848]

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.[1849]

[1845] *Ibid.*
[1846] *Ibid* at § 1798.125(a)(1).
[1847] *Ibid.*
[1848] *Ibid* at § 1798.145(a)(1)–(5).

Section 1798.81.5 (a) to (b) of the *California Civil Code (Customer Records):*[1850]

> 1798.81.5. (a) (1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.
>
> (2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license.
>
> (b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[1851]

Section 1798.82 (a) to (g) of the *California Civil Code (Customer Records):*[1852]

> 1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law

---

[1849] *Ibid.*
[1850] Cal Civ Code, 3 CIV 1.81 §1798.82 (2000) at § 1798.81.5(a)−(b) [*California Civil Code (Customer Records)*].
[1851] *Ibid.*
[1852] *Ibid* at § 1798.82(a)−(g).

enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that people whose information has been breached may take to protect themselves.

(C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

> (e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.
>
> (f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.
>
> (g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[1853]

European Union

Article 4(11) of the *GDPR*[1854] defines consent:

> Definitions
>
> (11) "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[1855]

Article 6(1) of the *GDPR:*[1856]

> Lawfulness of processing
>
> 1. Processing shall be lawful only if and to the extent that at least one of the following applies:

[1853] *Ibid* at § 1798.82(a)−(g).
[1854] *GDPR, supra* note 1790 at art 4(11).
[1855] *Ibid*.
[1856] *Ibid* at art 6(1).

> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.[1857]

Article 7 of the *GDPR:*[1858]

> Conditions for consent
>
> 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
>
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
>
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent,

---

[1857] *Ibid.*
[1858] *Ibid* at art 7.

> the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
>
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[1859]

Articles 33 and 34 of the *GDPR:*[1860]

> Article 33
>
> Notification of a personal data breach to the supervisory authority
>
> 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
>
> 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
>
> 3. The notification referred to in paragraph 1 shall at least:
>
> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
>
> 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

[1859] *Ibid.*
[1860] *Ibid* at arts 33−34.

> 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
>
> Article 34
>
> Communication of a personal data breach to the data subject
>
> 1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
>
> 2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
>
> 3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
>
> (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
>
> (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
>
> (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
>
> 4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.[1861]

Article 88(1) and (2) of the *GDPR:*[1862]

> Processing in the context of employment

[1861] *Ibid.*
[1862] *GDPR*, *supra* note 1790 at art 88(1)−(2).

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.[1863]

[1863] *Ibid.*

Appendix C: Privacy Provisions Analyzed in Chapter 4, Theme 3

Canada

Section 14 of *PIPEDA:*[1864]

> Hearing by Court
>
> Application
>
> 14 (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, in subsection 5(3) or 8(6) or (7), in section 10 or in Division 1.1.
>
> Time for application
>
> (2) A complainant shall make an application within one year after the report or notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.
>
> For greater certainty
>
> (3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).[1865]

Section 15 of *PIPEDA:*[1866]

> Commissioner may apply or appear
>
> 15 The Commissioner may, in respect of a complaint that the Commissioner did not initiate,
>
> (a) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;

[1864] *PIPEDA*, *supra* note 1766 at s 14.
[1865] *Ibid.*
[1866] *Ibid* at s 15.

(b) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or

(c) with leave of the Court, appear as a party to any hearing applied for under section 14.[1867]

Section 16 of *PIPEDA:*[1868]

Remedies

16 The Court may, in addition to any other remedies it may give,

(a) order an organization to correct its practices in order to comply with Divisions 1 and 1.1;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.[1869]

Section 17 of *PIPEDA:*[1870]

Summary hearings

17 (1) An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

Precautions

(2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.[1871]

Section 17.1 of *PIPEDA:*[1872]

Compliance agreement

[1867] *Ibid.*
[1868] *Ibid* at s 16.
[1869] *Ibid.*
[1870] *Ibid* at s 17.
[1871] *Ibid.*
[1872] *Ibid* at s 17.1.

> 17.1 (1) If the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 or 1.1 or a failure to follow a recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization.
>
> Terms
>
> (2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part.
>
> Effect of compliance agreement — no application
>
> (3) When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement,
>
> (a) shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and
>
> (b) shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions.
>
> For greater certainty
>
> (4) For greater certainty, a compliance agreement does not preclude
>
> (a) an individual from applying for a hearing under section 14; or
>
> (b) the prosecution of an offence under the Act.[1873]

Section 17.2(2) of *PIPEDA*:[1874]

> Agreement not complied with
>
> (2) If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for
>
> (a) an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or
>
> (b) a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result of an application made under paragraph 17.1(3)(b).[1875]

[1873] *Ibid.*
[1874] *Ibid* at s 17.2(2)

Section 28 of *PIPEDA:*[1876]

> Offence and punishment
>
> 28 Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of
>
> (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or
>
> (b) an indictable offence and liable to a fine not exceeding $100,000.[1877]

Section 52(1) to (4) of *BC PIPA:*[1878]

> Commissioner's orders
>
> 52 (1) On completing an inquiry under section 50, the commissioner must dispose of the issues by making an order under this section.
>
> (2) If the inquiry is into a decision of an organization to give or to refuse to give access to all or part of an individual's personal information, the commissioner must, by order, do one of the following:
>
> (a) require the organization
>
> (i) to give the individual access to all or part of his or her personal information under the control of the organization,
>
> (ii) to disclose to the individual the ways in which the personal information has been used,
>
> (iii) to disclose to the individual names of the individuals and organizations to whom the personal information has been disclosed by the organization, or
>
> (iv) if the organization is a credit reporting agency, to disclose to the individual the names of the sources from which it received personal information about the individual,

---

[1875] *Ibid.*
[1876] *Ibid* at s 28.
[1877] *Ibid.*
[1878] *BC PIPA, supra* note 1832 at s 52(1)−(4).

> if the commissioner determines that the organization is not authorized or required to refuse access by the individual to the personal information;
>
> (b) either confirm the decision of the organization or require the organization to reconsider its decision, if the commissioner determines that the organization is authorized to refuse the individual access to his or her personal information;
>
> (c) require the organization to refuse the individual access to all or part of his or her personal information, if the commissioner determines that the organization is required to refuse that access.
>
> (3) If the inquiry is into a matter not described in subsection (2), the commissioner may, by order, do one or more of the following:
>
> (a) confirm that a duty imposed under this Act has been performed or require that a duty imposed under this Act be performed;
>
> (b) confirm or reduce the extension of a time limit under section 31;
>
> (c) confirm, excuse or reduce a fee, or order a refund, in the appropriate circumstances;
>
> (d) confirm a decision not to correct personal information or specify how personal information is to be corrected;
>
> (e) require an organization to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of an organization to collect, use or disclose personal information;
>
> (f) require an organization to destroy personal information collected in contravention of this Act.
>
> (4) The commissioner may specify any terms or conditions in an order made under this section.[1879]

Section 53 of *BC PIPA*:[1880]

> Duty to comply with orders
>
> 53 (1) Not later than 30 days after being given a copy of an order of the commissioner, the organization concerned must comply with the order unless an application for judicial review of the order is brought before that period ends.

[1879] *Ibid.*
[1880] *Ibid* at s 53.

> (2) If an application for judicial review is brought before the end of the period referred to in subsection (1), the order of the commissioner is stayed from the date the application is brought until a court orders otherwise.[1881]

Section 56 of the *BC PIPA:*[1882]

> Offences and penalties
>
> 56 (1) Subject to subsection (2), an organization or person commits an offence if the organization or person
>
> (a) uses deception or coercion to collect personal information in contravention of this Act,
>
> (b) disposes of personal information with an intent to evade a request for access to the personal information,
>
> (c) obstructs the commissioner or an authorized delegate of the commissioner in the performance of his or her duties or powers under this Act,
>
> (d) knowingly makes a false statement to the commissioner, or knowingly misleads or attempts to mislead the commissioner, in the course of the commissioner's performance of his or her duties or powers under this Act,
>
> (e) contravenes section 54, or
>
> (f) fails to comply with an order made by the commissioner under this Act.
>
> (2) An organization or person that commits an offence under subsection (1) is liable,
>
> (a) if an individual, to a fine of not more than $10 000, and
>
> (b) if a person other than an individual, to a fine of not more than $100 000.
>
> (3) A person or organization is not liable to prosecution for an offence against this or any other Act because the person or organization complies with a requirement of the commissioner under this Act.
>
> (4) Section 5 of the Offence Act does not apply to this Act or the regulations.[1883]

Section 57(1) of the *BC PIPA:*[1884]

[1881] *Ibid*.
[1882] *Ibid* at s 56.
[1883] *Ibid.*

> Damages for breach of Act
>
> 57 (1) If the commissioner has made an order under this Act against an organization and the order has become final as a result of there being no further right of appeal, an individual affected by the order has a cause of action against the organization for damages for actual harm that the individual has suffered as a result of the breach by the organization of obligations under this Act.[1885]

Section 55 of the *QC Act:*[1886]

> 55. The Commission has all the powers necessary for the exercise of its jurisdiction; it may make any order it considers appropriate to protect the rights of the parties and rule on any issue of fact or law.[1887]
>
> The Commission may, in particular, order a person carrying on an enterprise to communicate or rectify personal information or refrain from doing so.

Section 58 of the *QC Act:*[1888]

> 58. A decision by the Commission becomes executory as a judgment of the Superior Court and has all the effects of such a judgment from the date of its homologation by the Superior Court.
>
> Homologation of the decision is obtained by the filing, by the Commission or one of the parties, of a true copy of the decision at the office of the clerk of the Superior Court of the district in which the domicile or the residence or business establishment of the person affected by the decision is situated.[1889]

Sections 91 to 93 of the *QC Act:*[1890]

> 91. Every person who collects, holds, communicates to third persons or uses personal information on other persons otherwise than in accordance with the provisions of Divisions II, III and IV of this Act is liable to a fine of $1,000 to $10,000 and, for a subsequent offence, to a fine of $10,000 to $20,000.

[1884] *Ibid* at s 57(1).
[1885] *Ibid*.
[1886] *QC Act, supra* note 1840 at s 55.
[1887] *Ibid*.
[1888] *Ibid* at s 58.
[1889] *Ibid.*
[1890] *Ibid* at ss 91−93.

However, for a contravention of section 17, the fine is $5,000 to $50,000 and, for a subsequent offence, $10,000 to $100,000.

92. Any personal information agent who contravenes any provision of section 70, 70.1, 72, 78 or 79 of this Act is liable to a fine of $6,000 to $12,000 and, for a subsequent offence, to a fine of $10,000 to $20,000.

92.1. Any person who hampers an inquiry or inspection by communicating false or inaccurate information or otherwise is guilty of an offence and is liable to a fine of $1,000 to $10,000 and, for a subsequent offence, to a fine of $2,000 to $20,000.

93. Where an offence under this Act is committed by a legal person, the administrator, director or representative of the legal person who ordered or authorized the act or omission constituting the offence, or who consented thereto, is a party to the offence and is liable to the prescribed penalty.[1891]

United States

Section 1798.155 (b) of the *California Consumer Privacy Act:*[1892]

1798.155. (b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.[1893]

European Union

Article 58 (1) and (2) of the *GDPR:*[1894]

Powers

1. Each supervisory authority shall have all of the following investigative powers:

[1891] *Ibid*.
[1892] *California Consumer Privacy Act*, *supra* note 1774 at § 1798.155(b).
[1893] *Ibid.*
[1894] *GDPR*, *supra* note 1790 at art 58(1)−(2).

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the

certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.[1895]

Article 83(1) to (6) of the *GDPR:*[1896]

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

[1895] *Ibid*.
[1896] *Ibid* at art 83(1)−(6).

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

> (d) any obligations pursuant to Member State law adopted under Chapter IX;
>
> (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
>
> 6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[1897]

Article 84(1) of the *GDPR*:[1898]

> Penalties
>
> 1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.[1899]

[1897] *Ibid*.
[1898] *Ibid* at art 84(1).
[1899] *Ibid*.

Curriculum Vitae

Name: Christina Lara Catenacci

Post-secondary Education:

Western Law, University of Western Ontario
London, Ontario, Canada
PhD

Osgoode Hall Law School, York University
Toronto, Ontario, Canada
LLM (Specialization in Labour and Employment Law)

Windsor Law School, University of Windsor
Windsor, Ontario, Canada
LLB

The University of Waterloo
Waterloo, Ontario, Canada
BA (Honours Psychology)

Related Work Experience:

Graduate Research Assistant
University of Western Ontario

Graduate Teaching Assistant
University of Western Ontario

Graduate Student Assistant
University of Western Ontario