Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?

Sarit K. Mizrahi

University of Ottawa, smizr100@uottawa.ca

Follow this and additional works at: https://ir.lib.uwo.ca/uwojls

Part of the Intellectual Property Law Commons, Privacy Law Commons, and the Torts Commons

Recommended Citation

Ontario’s New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?

Abstract
In the age of the Internet of Things, we are all susceptible to countless privacy violations. Society’s prevalent use of interconnected devices enables companies to collect and manipulate users’ personal data for their own monetary benefits. While the law grapples with how best to protect users from such privacy risks, another significant danger has emerged: by besting the often-weak security measures employed by companies that create interconnected devices, hackers can compromise the integrity of these electronics by remotely accessing them. This allows hackers to gain unauthorized access to the personal data of users and potentially hold their devices for ransom.

Smart devices are constantly evolving, and the risk that their users’ personal information will be misused is increasing. However, Ontario law has been slow to acknowledge the possibility for individuals to obtain damages for breaches of their privacy. To date, Ontario courts have only recognized two invasion of privacy torts: the Intrusion Upon Seclusion and the Public Disclosure of Private Facts, both of which are very limited in scope.

The aim of this paper is to examine whether these torts are sufficiently broad to address the privacy breaches that have become commonplace in our digital world. After outlining the privacy violations to which users of the Internet of Things are exposed, this paper will examine the potential of applying the Intrusion and Public Disclosure torts to such practices in an attempt to determine if users might be successful in obtaining monetary redress for such violations in a manner that the privacy legislation has been unable to achieve. This paper will then analyze whether or not these same torts might be used to impose liability on the companies responsible for personal information or devices that were breached by hackers. Finally, suggestions for how Ontario privacy law should evolve to better address our technologically enhanced reality will be explored.

Keywords
invasion of privacy, tort law, privacy law, Ontario

This article is available in Western Journal of Legal Studies: https://ir.lib.uwo.ca/uwojls/vol8/iss1/3
ONTARIO'S NEW INVASION OF PRIVACY TORTS: DO THEY OFFER MONETARY REDRESS FOR VIOLATIONS SUFFERED VIA THE INTERNET OF THINGS?

SARIT K. MIZRAHI

INTRODUCTION

Modern civilization’s increasing dependence on smart technology has created a surveillance society that treads dangerously close to an Orwellian dystopia.¹ There is, however, one acute difference: this society was not imposed upon us. Instead, we have chosen to forego our privacy for the mere sake of the convenience fostered by the devices running our lives.² With quotidian devices—from cell phones, to televisions, household appliances, and even children’s toys possessing Wi-Fi capabilities—the number of interconnected devices is expected to reach 34 billion by the year 2020.³ This phenomenon has become known as the Internet of Things.

In this age of the Internet of Things, we are susceptible to countless privacy violations. Every action performed by each user of an interconnected device generates a plethora of data points regarding their habits and preferences. Corporations are not only capturing this information, they are also storing,⁴ mining, manipulating, and disclosing this data to third parties for monetary gains.⁵ While the law has been grappling with how best to protect users from such privacy risks, another significant danger has arisen: malicious users who hack into corporate databases and overtake interconnected devices.

² Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, (New York: W.W. Norton & Company, 2015) at 51 [Schneier].
⁴ The storage of this information often occurs in the “cloud,” which is riddled with many of its own security vulnerabilities often manipulated by hackers (See Office of the Privacy Commissioner of Canada, The Internet of Things: An Introduction to Privacy Issues With a Focus on the Retail and Home Environments (Ottawa: Office of the Privacy Commissioner of Canada, 2016) at 21–22, online: <www.priv.gc.ca/media/1808/iot_201602_e.pdf>; Office of the Privacy Commissioner, Privacy and Cyber Security: Emphasizing Privacy Protection in Cyber Security Activities (Ottawa: Office of the Privacy Commissioner of Canada, 2014) at 1, online: <www.priv.gc.ca/media/1775/cs_201412_e.pdf>).
This danger is enabled by the often-weak security measures safeguarding these electronics.6

With technological advances increasing risks to user privacy, it is crucial to adequately protect this societal value from private corporations who continuously attempt to violate it.7 This being a rather controversial remark, we will immediately dispel of some of the main arguments used by opponents of more robust privacy protections, though it is beyond the scope of this paper to address them all.8 The first is that privacy is not necessary if you have nothing to hide. Rare is the person who can support this position, as elicited by the following examples: “One has only to start asking questions about ‘How much money do you have in your bank account?’”; “Have you ever had psychiatric care?”; or, “Have you ever had an abortion?”; and people quickly discover, “Well, I do have some sense of privacy in the form of a fair amount of information about myself that I prefer to keep under my control.”9

The second proposition often put forth by adversaries of stronger privacy protections is that such protections are impractical to implement and enforce through the legal system. While this is a valid concern, market self-regulation has proven inadequate and thus, “it is unrealistic to expect privacy to be adequately protected in the absence of [legislative] intervention.”10 Although privacy legislation often acts as a reactive solution against corporations that misuse users’ personal information, and may therefore not be sufficient to protect privacy on its own, legislation is part of a grander scheme “that combines consumer education, user empowerment, and selective enforcement of existing targeted laws and other legal standards (torts, anti-fraud laws, contract laws, and so on).”11 This comprehensive approach “can strike a reasonable balance between information sharing, online commerce, and personal privacy in an information marketplace characterized by rapid technological change and constantly evolving norms.”12 Additionally, this framework is able to better guide the personal

7 The societal importance of privacy has been confirmed by the Supreme Court of Canada on several occasions (See generally Hunter v Southam Inc, [1984] 2 SCR 145; R v Dyment, [1988] 2 SCR 417; R v Tessling, [2004] 3 SCR 432 [Tessling]; Hill v Church of Scientology of Toronto, [1995] 2 SCR 1130; R v O’Connor, [1995] 4 SCR 411).
8 For a more exhaustive discussion, see: Julie E Cohen, “What Privacy is For?” (2013) 124 Harv L Rev 1904 [Cohen].
9 David H Flaherty, “Some Reflections on Privacy and Technology” (1998) 26 Man LJ 219 at 220; See also Tessling, supra note 7; James Grimmelmann, “Privacy as Product Safety” (2009) 18 Widener LJ 793 at 797–800 (discussing a study disclaiming the common myth that Facebook users don’t care about their privacy).
12 Ibid at 414.
information handling practices of private corporations, thus equally playing a preventative role. The challenge of enforcing privacy legislation, therefore, does not mean “that society is entirely powerless to address [privacy] through legal or regulatory means.”13 Perhaps privacy regulation is not as efficient as we might like as a singular solution, and perhaps individuals who are particularly sensitive about their online privacy will be obliged to compliment it with other measures,14 but this solution still provides a certain level of privacy protection that would otherwise be absent and therefore serves an important purpose.

A corollary to this second viewpoint is that, because people can exercise their own will of what to share online, any intervention on behalf of the government would unnecessarily interfere with the individual liberty and autonomy of its citizens. The problem with this position is that “[i]t’s not about what we know we’re sharing, it’s about what we don’t know is being collected and sold about us.”15 Information that users believe to be private is being used to create psychological profiles employed to target these individuals with advertisements and even surreptitiously influence their life choices,16 behaviours, and self-perception;17 as such, the government’s interference cannot be considered to impose undue limitations on the freedom of their citizens. Rather, viewed through this lens, any intervention on behalf of the government must be construed as restricting companies in their exploitation of citizens18 and safeguarding our democratic society by furthering “autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power.”19

Finally, the last position frequently maintained against stronger privacy protections in the digital era is that people who do not like being subjected to “dataveillance” should not use the Internet. Security expert Bruce Schneier puts it in the following manner:

13 Ibid at 412.
14 Ibid.
16 Hannes Grassegger & Mikael Krogerus, “The Data That Turned the World Upside Down”, Motherboard Vice (28 January 2017), online: <www.motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win/> (discussing how this type of personal information was used to influence American users to favour Donald Trump during the last United States election).
18 Cohen, supra note 8.
“[this] advice is not practical. It’s not reasonable to tell people that if they don’t like the data collection, they shouldn’t e-mail, shop online, use Facebook, or have a cell phone. I can’t imagine students getting through school anymore without Internet search or Wikipedia, much less finding a job afterwards. These are the tools of modern life. They’re necessary to a career and a social life. Opting out just isn’t a viable choice for most of us, most of the time; it violates what have become very real norms of contemporary life.”

Despite the impracticality of escaping the Internet in an era defined by smart technology, the only statutory privacy protections available to Ontario citizens are enshrined in the Personal Information Protection and Electronic Documents Act\(^\text{21}\) ("PIPEDA"), Canada’s federal private-sector privacy law. Compliance with PIPEDA, as well as the Privacy Act covering federal government departments’ and agencies’ personal information handling practices, is overseen by the Privacy Commissioner of Canada, whose role is to protect and promote the privacy rights of individuals.\(^\text{22}\) When it comes to ensuring PIPEDA compliance, the Privacy Commissioner may investigate all complaints lodged by individuals regarding the information handling practices of private companies in any Canadian province that has not adopted substantially similar privacy legislation. To date, the only Canadian provinces that have adopted similar privacy legislation are Quebec, British Columbia and Alberta.\(^\text{23}\) However, despite being given the mandate to investigate such complaints, the Commissioner is not endowed with the power to grant compensation to the complainant.\(^\text{24}\) While the statute provides individuals with the option to pursue the matter further in the Federal Court,\(^\text{25}\) “damage awards are extremely rare and are limited to the most egregious situations.”\(^\text{26}\) In addition to these legislative limitations,\(^\text{27}\) Ontario tort law has also only slowly acknowledged damages for privacy breaches due to the nature of the common law.

\(^{20}\) Schneier, \textit{supra} note 2 at 60-61; see also Adam Pabarcus, “Are ‘Private’ Spaces on Social Networking Websites Truly Private? The Extension of Intrusion Upon Seclusion” (2011) 38 Wm Mitchell L Rev 397 (“A common sense response to such concerns is that if people are truly concerned about such information getting out, they simply should not post it on social networking websites… [however] if someone wishes to share information with a certain group and takes measures to create seclusion from others, that space should be recognized as private by the law” at 410).

\(^{21}\) SC 2000, c 5 [PIPEDA].


\(^{23}\) \textit{Ibid.}


\(^{25}\) \textit{PIPEDA, supra} note 21 at s 16(c).

\(^{26}\) Jared A Mackey, “Privacy and the Canadian Media: Developing the New Tort of ‘Intrusion Upon Seclusion’ with Charter Values” (2012) 2:1 UWO J Leg Stud 3 at 3 [Mackey]; see also \textit{Randel v Nabodys Fitness Centres}, 2010 FC 681 at paras 55, 56.

\(^{27}\) See Office of the Privacy Commissioner of Canada, \textit{The Case for Reforming the Personal Information Protection and Electronic Documents Act}, (Ottawa: May 2013) at 5–10, online:
The Ontario judiciary’s move towards the recognition of a privacy tort began over a century ago\textsuperscript{28} in an effort to address technological change. This evolution culminated in the Ontario Court of Appeal’s decision in \textit{Jones v Tsige}.$^{29}$ In this landmark case, the plaintiff’s banking records were surreptitiously accessed by her ex-husband’s new partner. The Court noted “the pressing need to preserve ‘privacy’ which is being threatened by science and technology to the point of surrender,”\textsuperscript{30} and chose to develop the common law “to respond to the problem posed by the routine collection and aggregation of highly personal information […] readily accessible in electronic form.”\textsuperscript{31} In this case, the tort of Intrusion Upon Seclusion (“Intrusion”) was adopted because the facts of this case “[cried] out for a remedy.”\textsuperscript{32} Intrusion imposes liability on a person that intentionally or recklessly intrudes, physically or otherwise, upon the seclusion of another or their private affairs or concerns without lawful justification, given the invasion would be highly offensive to a reasonable person.\textsuperscript{33}

Several years following this decision, the Ontario Superior Court of Justice tried the case of \textit{Doe 464533 v ND}.$^{34}$ This case revolved around an intimate video of a woman posted on a pornographic website by her ex-boyfriend without her knowledge or consent.$^{35}$ This case marks the first in Canada where a victim sought civil damages for what is commonly termed “revenge porn.”$^{36}$ The Court recognized “the devastating harm that can result from these acts, ranging from suicides by teenage victims to career-ending consequences when established persons are victimized.”$^{37}$ Accordingly, the Court chose to further develop the common law to address this unfortunate phenomenon through the tort of Public Disclosure of Private Facts (“Public Disclosure”). This tort maintains that “[one] who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other’s privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.”$^{38}$ The future of

\begin{itemize}
\item<www.priv.gc.ca/media/1324/pipeda_r_201305_e.pdf>;
\item\textit{Jones v Tsige}, 2012 ONCA 32 at para 67 [\textit{Jones}].
\item\textit{Ibid}.
\item\textit{Jones, supra} note 28 at para 68.
\item\textit{Ibid} at para 69.
\item\textit{Ibid} at para 70.
\item2016 ONSC 541 [\textit{Doe}].
\item\textit{Ibid} at para 1.
\item\textit{Ibid} at para 18.
\item\textit{Ibid} at para 16.
\item\textit{Ibid} at para 46.
\end{itemize}
this tort in Ontario is uncertain because the default judgment recognizing it was recently set aside. However, given the judiciary’s willingness to recognize invasion of privacy torts, this tort may continue to be recognized. This paper will therefore address each of the torts of Public Disclosure and Intrusion.

The formulation of both invasion of privacy torts is based on William Prosser’s seminal article on privacy, which American law has enacted through its Restatement of Torts. American scholars are divided on the applicability of these torts to modern privacy invasions. The overwhelming majority maintains that these torts are not applicable to modern privacy violations, given the judiciary’s repeated refusal to apply them to informational privacy breaches. A small minority contends that the torts’ broad phrasing demonstrates potential to evolve towards such applications, should the courts choose to permit them.


Restatement (Second) of Torts § 652B, 652D (Am Law Inst 2010).

Alec Wheatley, “Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation With a Private Right of Action” (2015) 45 Golden Gate UL Rev 265 (“For example, these torts are not equipped to deal with informational privacy, because they are concerned with a person’s ‘interest in solitude’ … There is a need for legislation that can adequately address the intricacies of how consumers expect their information to be handled. This requires a subtlety that the four original privacy torts are unable to furnish” at 271); Jason A Kotzker, “The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad” (2002) 15 St Thomas L Rev 727 (these torts “[place] a lofty burden on the plaintiff to prove that the collection and dissemination of personal preferences gathered via on-line advertising firms are, in fact, highly offensive to the reasonable person” at 732-733); See also Andrea M Matwyshyn, “Privacy, the Hacker Way” (2013) 87:1 S Cal L Rev 1 at 36-38; Maayan Y Vodovis, “Note, Look Over Your Figurative Shoulder: How to Save Individual Dignity and Privacy on the Internet” (2012) 40 Hofstra L Rev 811 (“These torts ‘are largely incapable of remedying the intrusiveness’ of increasingly invasive technologies’ at 817) [Vodovis]; Josh Blackman, ‘Omnivillaince, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual’s Image over the Internet” (2009) 49 Santa Clara L Rev 313 at 314; Patricia Sánchez Abril, “Recasting Privacy Torts in a Spaceless World” (2007) 21 Harv J L & Tech 1 at 12; Neil M Richards & Daniel J Solove, “Prosser’s Privacy Law: A Mixed Legacy” (2010) 98 Calif L Rev 1887 at 1921; Kelsey Maxwell, “The Pros and Cons of Regulation and Suggestions for Adherence to California’s Constitutional Right to Privacy” (2013) 19 NEXUS 51 (“This article, on the other hand, focuses on the commercial use and indirect dissemination of private information through advertising. This practice does not fit very well into Prosser’s tort for public disclosure of private facts” at 53).

Alexander H Tran, “The Internet of Things and Potential Remedies in Privacy Tort Law” (arguing that the elements required to prove torts of intrusion upon seclusion and public disclosure of private facts are sufficiently broad to be interpreted to apply to the types of privacy invasions experienced through the Internet of Things, only if the courts are willing to extend them in this manner); Jane Yakowitz Bambauer, “The New Intrusion” (2012) 88 Notre Dame L Rev 205 (“The tort of intrusion upon seclusion offers the best theory to target legitimate privacy harms in the information age” at 205) [Yakowitz Bambauer]; Adam Thierer, “The Internet of Things and Wearable Technology: Addressing Privacy and
The Canadian formulation of the Intrusion and Public Disclosure torts attempts to avoid similar drawbacks by closely tracking them on the right to informational privacy.\(^6\) However, the application of each of the torts is subject to multiple contradictory interpretations that cast doubt on their ability to extend protections to modern “dataveillance” practices.\(^7\) After outlining the digital privacy risks associated with the routine aggregation of interconnected device users’ personal information by private companies, this paper will examine the potential of applying the Intrusion and Public Disclosure torts to such practices in an attempt to determine if users might be successful in obtaining monetary redress for such violations in a manner that PIPEDA has been unable to achieve. The paper will then examine whether or not these same torts might be used to impose liability on the companies responsible for personal information or devices that were breached by hackers. Finally, the conclusion provides suggestions for how Ontario privacy law can evolve to better address our technologically enhanced reality.

I. THE INTERNET OF THINGS VS. PRIVACY: WHAT IS AT RISK?

Due to the novel territory of electronic personal information, the associated risks are often misconstrued, leaving many users to perceive that the convenience afforded by their interconnected devices outweigh their claims to informational privacy. Not only are these users subjected to corporations collecting, mining, and manipulating their personal data for monetary gains, they are also exposed to the risks of malicious users obtaining unauthorized access to that information and using it for illicit purposes.

Personal Data as Currency: The Monetary Value of Behavioural Data and What This Means for Users

Prior to the advent of the Internet, Professor Arthur Miller foretold the creation of an “information buddy system” which would “result in a subterranean information exchange network that functions on a mutual backscratching basis or can be invoked for

\(^6\) Jones, supra note 28 at para 66.

\(^7\) Although inappropriate uses of data collected via interconnected devices may give rise to pursuits in virtue of other torts, such as negligence, breach of confidence, conversion, trespass to property, or intentional infliction of emotional distress, they are very difficult to prove and will likely fail to offer users of such devices with any protection (Chris Dockrill, “Computer Data Banks and Personal Information: Protection Against Negligent Disclosure” (1987) 11 Dalhousie LJ 546; Jacqueline D. Lipton, “We, the Paparazzi: Developing a Privacy Paradigm for Digital Video” (2010) 95 Iowa L Rev 919 at 932-933 [Lipton]; Dustin D Berger, “Balancing Consumer Privacy With Behavioral Targeting” (2011) 27 Santa Clara Computer & High Tech L J 3 at 35) [Berger].
Nearly fifty years later, this prediction has come to fruition. Companies use data harvesting technologies to aggregate the sensitive personal information of billions of interconnected device users, and use the information as a form of currency. Companies’ substantial interest in user behavioural data is predicated on a single goal: effective advertising. Gaining access to data about consumers' preferences allows companies to more effectively use targeted advertising, increasing the chances that their products will be purchased.

The prevalent use of portable smart devices within interconnected environments has exponentially increased the amount of users’ personal details that are captured. When all of this personal data is coupled with the continuous development of mass surveillance technologies, we are left with an ingenious scheme that facilitates targeted advertising goals of corporations. Companies can access an uncanny amount of user data in this fashion—ranging from general information, such as age and occupation, to more discrete details, including sexual preferences, financial standing, health status, and much more. This reality raises the assertion that companies may know users better than

---

49 For example, Web Cookies (a small file stored on a user’s computer so that websites can recognize them and track their preferences (“Definition of: Cookie” PCMag, online: <www.pcmag.com/encyclopedia/term/40334/cookie>)), Flash Cookies (these are similar to web cookies but they can hold significantly more data and they are stored in a part of the computer where they will not be erased if web cookies are deleted from a user’s browser (“Definition of: Flash cookie” PCMag, online: <www.pcmag.com/encyclopedia/term/62745/flash-cookie>)), Deep-Packet Inspection (technology that analyzes the content of any data sent via the Internet (“Definition: Deep Packet Inspection” PCMag, online: <www.pcmag.com/encyclopedia/term/58470/deep-packet-inspection>)), WiFi Positioning System (the use of WiFi signals to determine the location of a particular interconnected device (“Wi-Fi Positioning System” Techopedia, online: <www.techopedia.com/definition/27532/wi-fi-positioning-system>)), Global Positioning System (the use of satellite signals to determine the location of an interconnected device (“Definition: GPS” PCMag, online: <www.pcmag.com/encyclopedia/term/43884/gps>)), Biometric Recognition Technology (technology that uses a person’s unique biological traits, such as facial features or voice, to identify them in any environment (FIDIS, “Use and Abuse of Biometric Data and Social Networks” FIDIS, online: <www.fidis.net/resources/identity-use-cases-scenarios/use-and-abuse-of-biometric-data-and-social-networks/>).
51 Schneier, supra note 2 at p. 47.
52 Manwaring, supra note 5 at 11.
53 See Mizrahi, supra note 50 at p 9-63.
they know themselves.\textsuperscript{54}

The list of personal information available to corporations is growing with continuous advances in technology. Wi-Fi and GPS enabled mobile devices provide corporations with real-time location information, which allows advertising to users in a timely manner.\textsuperscript{55} As if being followed through one’s daily activities is not sufficiently invasive, a new assortment of Internet connected sex toys gives an entirely novel meaning to invasions of intimate affairs: one such device automatically sent the manufacturer “real-time digital notes on how [customers] responded to ‘pulse’ mode compared to ‘cha cha.’”\textsuperscript{56}

The adoption of biometric recognition technology further enables large, web-based companies such as Google and Facebook to identify individuals in both virtual and physical spheres through their unique biological traits, such as their facial features\textsuperscript{57} or the sound of their voice.\textsuperscript{58} Other devices, such as Smart TVs or Smart Home Assistants, employ voice recognition technology that enable users’ conversations to be captured in the privacy of their own homes.\textsuperscript{59} Users are assured that these devices are not “always-on” and that interactions are only recorded when the trigger word is used; however, the use of the word may be outside the owner’s control, which may result in inadvertent recording. A recent Burger King ad exemplifies this risk by using the trigger words “O.K. Google” to activate and instruct Google’s Home device to inform users about the Whopper Sandwich.\textsuperscript{60}


\textsuperscript{55} Schneier,\textit{ supra} note 2 at 47-49; David Booth, “Privacy Could be a Steep Price for Convenience: A Vehicle’s Connectivity Opens Up a Wealth of Information to Automakers”, \textit{The Ottawa Citizen} (6 January 2017), online: <www.pressreader.com/canada/ottawa-citizen/20170106/282114931254182>.


\textsuperscript{57} Anne T McKenna, “Pass Parallel Privacy Standards or Privacy Perishes” (2013) 65:4 Rutgers Law Rev 1041 at 1067.


These self-imposed wiretaps present far greater risks than those posed by creative advertisements. Prosecutors in Arkansas recently made a controversial attempt to gain access to voice recordings captured by a murder suspect’s Amazon Echo device.⁶¹ Although Amazon refused to acquiesce to this demand, the fact remains that Amazon potentially had possession of a recording that could have implicated or exonerated their customer in a murder. In addition to having severe implications for the liberty of individuals, Amazon’s aggregation of such information presents a multitude of other consequences should this data not be protected. These consequences can include being subject to wrongful use and breaches by hackers or targeting consumers with advertising.

The examples highlighted above represent a mere sample of the myriad privacy violations that digital users are subjected to daily. “Dataveillance’s” implications extend well beyond privacy deprivation and potential human rights violations. Essentially, “[mass surveillance] enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free.”⁶² Despite these serious risks, users are endowed with limited legal avenues for the pursuit of companies that violate their privacy, as Part II will address.⁶³

**The Modern Version of a Holdup: Hacking the Security Flaws of Corporate Databases and Interconnected Devices**

Malicious users have come to embody the petty criminals of the information age, hacking a diverse range of internet connected devices from sophisticated computer systems⁶⁴ to children’s toys.⁶⁵ Malicious users exploit the security flaws of interconnected devices for any number of illicit purposes, giving age-old felonies a modern twist. Car jacker no longer need to physically slide open a car door’s lock with a coat hanger and speedily hot-wire the vehicle to drive off before getting caught. In this digital age, cars are “stolen” while still in your driveway. Hackers deactivate the Wi-Fi enabled computers of New Age cars using ransomware and render the vehicles useless.

---


⁶³ See below, p. 12-28.


until a ransom is paid in Bitcoins. This is a clever crime for potential perpetrators; they steal and make mounds of untraceable cash, all without leaving the comfort of their own home.

Replace the car in this tale with just about any other interconnected device, and there is bound to be a parallel. Smart TVs have been held for ransom while their activated voice recognition allowed malicious users to spy on their victims. Corporate databases have been hacked—not only allowing malicious users to access the mountains of personal user data accumulated by these companies but also allowing hackers to steal sensitive personal information. In many instances, hackers used the stolen credit card details and social insurance numbers of millions of users for identity theft purposes. Even more disturbing is the recent hacking of Wi-Fi enabled baby monitors, where hackers were able to converse with babies at bedtime and say any number of inappropriate things. The examples are endless.

These flagrant privacy violations pose serious risks to users of interconnected devices, yet individuals are largely unable to protect themselves. Instead, users tend to rely entirely on the corporations that collect their data and create their devices. While the law obliges these companies to protect the information and devices against unauthorized access, the reality is that the steps taken are often insufficient to abolish the security flaws exploited by malicious users.

66 Bitcoins are a form of untraceable currency that people can barter with anonymously (Tal Yelling, Dominic Aratari, and Jose Pagliery, “What is Bitcoin?” CNNMoney, online: <www.money.cnn.com/infographic/technology/what-is-bitcoin>).
authorities, users are often left without a sufficient legal remedy for this serious invasion of their privacy.

II. INTRUSION UPON SECLUSION VS. PUBLIC DISCLOSURE OF PRIVATE FACTS: DO THEY EMPOWER USERS TO ENFORCE THEIR PRIVACY RIGHTS AGAINST COMPANIES?

The tort of Intrusion is concerned with unauthorized intrusions such as “listening or looking, with or without mechanical aids, into [a person’s] private affairs” regardless of whether the data is disseminated. Conversely, the tort of Public Disclosure addresses the publication of private facts irrespective of an intrusion. While companies’ use of “dataveillance” technologies would certainly qualify as intentional intrusions, their ability to engage the tort of Intrusion is not guaranteed. Similarly, although ordinary citizens’ behavioural data is unlikely to be of legitimate public interest, the applicability of the tort of Public Disclosure to the use of such data for targeted advertising is uncertain.

The vagueness of the criteria required to establish each of the invasion of privacy torts can result in multiple contradictory interpretations, making it difficult to state with certainty whether either tort can apply to privacy violations arising from the Internet of Things. This ambiguity arises out of three primary sources. First, it is unclear

---

73 Jones, supra note 28 at para 20.
75 Jones, supra note 28 at para 71.
76 According to the Supreme Court of Canada in Grant v Torstar Corp., “[to] be of public interest, the subject matter ‘must be shown to be one inviting public attention, or about which the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached’” (Grant v Torstar Corp., 2009 SCC 61, [2009] 3 SCR 640 at para 105, citing Raymond E Brown, The Law of Defamation in Canada, vol. 2 (Scarborough: Carswell, 1999 (loose-leaf updated 2008, release 3)) at p 15-137, 15-138). The Court then goes on to specify that “the public interest is not synonymous with what interests the public. The public’s appetite for information on a given subject […] is not on its own sufficient to render an essentially private matter public […]” (Grant v Torstar Corp, ibid at para 102) because “mere curiosity or prurient interest is not enough. Some segment of the public must have a genuine stake in knowing about the matter published” Grant v Torstar Corp, ibid at para 105). In this light, we do not believe it is likely for the behavioural data of ordinary users of interconnected devices would be considered as a matter of public interest. For a deeper analysis regarding what is in the public interest, see Mackey, supra note 26 at 12; see also Bryan T McKinney and Dwayne Whitten, “Arkansas Surfers and Their Privacy, or Lack Thereof: Does the Common Law Invasion of Privacy Tort Prohibit E-Tailers’ Use of ‘Cookies’?” (2002) 23 UALR L Rev 751 at 773 [McKinney & Whitten].
whether the behavioural data aggregated through interconnected devices is encompassed by the terms “private affairs or concerns”78 and “private facts.”79 Second, it is questionable whether the consent acquired by the companies collecting this data is sufficient lawful justification80 or authorization81 to preclude the application of the Intrusion and Public Disclosure torts. Finally, it is debatable whether the intrusions or data disclosed in digital environments can be considered “highly offensive to a reasonable person,”82 particularly given that these violations have become commonplace in our society.

Private Affairs or Concerns and Private Facts: Do These Terms Encompass the Behavioural Information Gathered Through Corporate “Dataveillance”?

The tort of Intrusion will only be available to individuals whose “private affairs or concerns” are invaded.83 Although the Jones decision does not provide much guidance regarding what fulfills this criterion, the Court specified that “it is only intrusions into matters such as one’s financial or health records, sexual practises and orientation, employment, diary or private correspondence”84 that will amount to “deliberate and significant invasions of personal privacy.”85 Conversely, the Public Disclosure tort is only accessible where someone’s “private facts” are publicized.86 While any facts in the public domain are excluded from this definition, the Doe decision clarifies that “private facts” also includes information related to

[...] phases of [someone’s] life and [...] activities and some facts about himself that he does not expose to the public eye, but keeps entirely to himself or at most reveals only to his family or to close friends. Sexual relations, for example, are normally entirely private matters, as are family quarrels, many unpleasant or disgraceful or humiliating illnesses, most intimate personal letters, most details of a man’s life in his home, and some of his past history that he would rather forget.87

The question is whether the terms “private affairs or concerns” and “private facts” encompass behavioural data aggregated in digital environments such that users

---

78 Jones, supra note 28 at para 71.
79 Doe, supra note 34 at para 46.
80 Jones, supra note 28 at para 71.
81 Doe, supra note 34 at para 44.
82 Ibid at para 46; Jones, supra note 28 at para 71.
83 Jones, supra note 28 at para 71.
84 Ibid at para 72.
85 Ibid.
86 Doe, supra note 34 at para 46.
87 Ibid at para 42.
would have a privacy tort claim. The “obviously private approach” adopted in *Jones* and *Doe* makes it clear that sensitive information—such as data regarding sexual preferences, financial standing, or illnesses—will undoubtedly fall under the ambit of these terms. However, considering that “claims from individuals who are sensitive or unusually concerned about their privacy are excluded,” it is questionable whether less intimate personal data amassed by companies will suffice to establish these elements.

Unfortunately, the Canadian decisions on invasion of privacy torts provide little direction to guide this analysis. The repeated endorsement of the *Restatement* model in Canadian courts, however, suggests that the American discourse may be enlightening. The American courts use a bifurcated empirical approach holding that “what is public is not private and what is private is not public.” In the United States, the torts of Intrusion and Public Disclosure only protect secret affairs, concerns or facts that are secluded from public scrutiny, or instances where steps have been taken to maintain one’s privacy. The application of these torts has therefore rarely been extended to the protection of informational privacy, leading to the conclusion that people possess no

---

90 *Jones*, supra note 28 at para 72.
91 Hunt, supra note 88 at 675.
92 Ibid at 682.
93 Vera Bergelson, “It’s Personal But is it Mine? Toward Property Rights in Personal Information” (2003) 37 UC Davis L Rev 379 at 407-408; see also Nancy J King, “Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices” (2008) 60:2 Fed Comm LJ 229 (“Because both the tort of unreasonable intrusion into seclusion and the tort of public disclosure of private facts require the plaintiff to prove private facts that underlie the claimed privacy invasion, courts are unlikely to apply these torts to address consumers’ privacy claims associated with commercial surveillance or other collection and use of consumers’ personal data […]” at 295) [King].
94 See *United States v Gines-Perez*, 214 F Supp (2d) 205 at 225 (DPR 2002); *Konop v Hawaiian Airlines Inc*, 302 F (3d) at 884 (9th Cir 2002); *Yath v Fairview Clinics*, 767 NW (2d) 34 at 51 (Minn Ct App 2009) (Johnson, J., concurring); *Pietrylo v Hillstone Restaurant Group*, Dockey No 06-5754 (DNJ 2008) [Pietrylo]; see also Pabarcus, supra note 20 at 423.
claim to privacy on the Internet because it is primarily a public arena. Several scholars have labelled the refusal to recognize a degree of privacy within public spheres as nonsensical, especially in the digital age. Essentially, “defining private by contrasting it with public assumes that the dividing line between the two concepts is clear, when in reality they are not ‘mutually exclusive categories but matters of degree, existing on a continuum.’”

Despite drawing upon the American model, there are two reasons that the Intrusion and Public Disclosure torts’ application to digital environments is less likely to be limited by a bifurcated approach in Canada. The first is founded on the statement in Jones that “the right to informational privacy closely tracks the same interest that would be protected by a cause of action for intrusion upon seclusion.” The decision then proceeds to mention PIPEDA as one of the Canadian laws protecting the right to informational privacy, among others. Since the information aggregated by companies online is the type of private information that is subject to PIPEDA regulation, this legislation’s definition of personal information could serve as a basis for the types of “private affairs or concerns” and “private facts” that could potentially be protected by the Intrusion tort in the context of corporate “dataveillance.”

PIPEDA’s definition of private information includes all personally identifiable information. Although this definition lacks precision, case law calls for an expansive interpretation of personal data, which covers any information that merely allows for

---

96 Bryce Clayton Newell, “Rethinking Reasonable Expectations of Privacy in Online Social Networks” (2010) 17 Rich JL & Tech 1 at 21; see also Boring v Google Inc, ibid (refusing to apply the tort of Intrusion to the pictures available in Google Street View, even though they entered a private road with a “do not enter” sign to acquire said images); United States v Hambrick, ibid (refusing to recognize any privacy interest in the subscriber information of Internet users); Daniel J Solove, The Digital Person: Technology and Privacy in the Information Age (New York: New York University Press, 2004); Sovern, ibid at 1317-18; Ybarra, ibid at 274.
99 Ibid at 675.
100 Jones, supra note 28 at para 66.
101 Ibid.
103 PIPEDA, supra note 21, s 2(1).
104 Dagg v Canada (Minister of Finance), [1997] 2 SCR 403, J Laforest dissenting at para 68; Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 SCR 66 at para 23; Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157.
the possibility of identifying an individual.\textsuperscript{105} While non-sensitive behavioural data collected in virtual environments may not be enough to identify someone, it “may be linked or merged with the [personally identifiable information] of these users”\textsuperscript{106} such that they are always identifiable.\textsuperscript{107} If private affairs, concerns, or facts will conform to PIPEDA’s definition of personal data, the Intrusion and Public Disclosure torts may extend protection to informational privacy in interconnected environments.

The second reason the Canadian adaptation of these torts may avoid the application of the private/public dichotomy is that Canadian courts, including the Supreme Court of Canada, have recognized that privacy can be invaded in the public sphere.\textsuperscript{108} This acknowledgment addresses the lack of clear delineation between what is public and private, especially in the digital age.\textsuperscript{109} Canadian law is therefore endowed with the necessary flexibility to recognize that the Internet is not merely a public arena, but a public arena that utilizes enhanced technologies to reveal personal details in an unprecedented manner.

This approach enables Canadian law to address egregious privacy concerns of the Internet of Things that would otherwise not be actionable in the United States. This can be illustrated by an example involving Facebook. When a user uploads a photo to this social network, Facebook's software records the unique facial features of every individual in that picture; each of these people then becomes identifiable in any subsequent photos that may be uploaded by themselves or other people. This feature eliminates the freedom of remaining anonymous when one is unexpectedly captured in a photograph in public.\textsuperscript{110} The American bifurcated approach to private facts is unable to respond to the intricacies involved in the aforementioned example. Therefore, individuals in the United States enjoy “little legal recourse in stopping photos from being uploaded onto Facebook and [their] facial biometrics from being exploited


\textsuperscript{109} Paton-Simpson, supra note 98 at 324; McClurg, supra note 98 at 1041.

\textsuperscript{110} Vodovis, supra note 44 at 819; Kane, supra note 74 at 355; Lipton, supra note 47 at 927.
Conversely, the Canadian view that certain circumstances support the recognition of privacy in public places may favour a contextual approach to such situations that will better protect users against the misappropriation of their biometric features.

Despite the endorsement of the American model in both the Jones and Doe decisions, the more rigid approach to “private affairs,” “concerns,” and “private facts” may still be avoided by the Canadian application of the Intrusion and Public Disclosure torts. The Canadian stance that privacy torts protect the interests of informational privacy, and that privacy can exist in public forums, supports this position. While this viewpoint may promote recognizing some non-sensitive behavioural data as private for privacy tort purposes, their consideration as such remains to be seen. Furthermore, the “highly offensive” criterion\(^\text{112}\) may provide another avenue to distinguish between sensitive and non-sensitive data.

**Intrusion Without Lawful Justification and Unauthorized Public Disclosure: Is User Consent Enough to Preclude Privacy Tort Claims?**

Whereas the Intrusion tort will be unavailable to individuals whose privacy was invaded with lawful justification,\(^\text{113}\) the Public Disclosure tort will be unavailable to people who authorized the publicity of their information.\(^\text{114}\) To a certain extent, authorization and lawful justification are intrinsically linked: if the former exists, so will the latter. As such, user consent to collect and disclose personal data will suffice to preclude application of both torts. While American privacy claims “can be defeated by consent, including consent that was improperly induced,”\(^\text{115}\) the Canadian approach provides the opportunity to avoid such outcomes. In Canada, consent is conceived differently for informational privacy purposes and for tort actions. Considering the

---

\(^{111}\) Jonathan Shaw, “FACEbook Confidential: The Privacy Implications of Facebook’s Surreptitious and Exploitative Utilization of Facial Recognition Technology” (2012) 31 Temple J Science Technology & Environmental L 149 at 159.; see also Note, In The Face of Danger: Facial Recognition and the Limits of Privacy Law, (2007) 120 Harv L Rev1870 at 1876-77 (“As may already be apparent, [intrusion and public disclosure] are inapplicable to those whose photos are taken in public spaces and then uploaded to the Internet. […] The fact that an image is snapped at a party, a restaurant, a park, or a bar dooms the claim. As one judge observed about intrusion, the tort simply [does] ‘not apply to matters which occur in a public place or a place otherwise open to the public eye.’” (citing Fogel v Forbes, Inc., 500 F Supp 1081, 1087 (ED Pa 1980)).

\(^{112}\) See below, p 22.

\(^{113}\) Jones, supra note 28 at para 71.

\(^{114}\) Doe, supra note 34 at para 44.

Jones decision’s contention that privacy torts protect informational privacy interests, both versions of consent must be considered.\textsuperscript{116}

The first framework to consider is consent under informational privacy legislation. The form of consent required by this legislation is dependent on the type of behavioural advertising at stake. For online interactions, consent is regulated by PIPEDA,\textsuperscript{117} which maintains that meaningful consent must be acquired to collect and use personal information.\textsuperscript{118} For consent to be meaningful, companies must state their purposes “in such a manner that the individual can reasonably understand how the information will be used or disclosed.”\textsuperscript{119} The form of consent must be reasonable in light of the data’s sensitivity;\textsuperscript{120} implicit consent will only be acceptable in situations that satisfy strict criteria.\textsuperscript{121} PIPEDA therefore requires the adoption of a contextual approach when determining the form consent should take under particular circumstances.\textsuperscript{122}

Despite PIPEDA’s seemingly strict consent requirements, the ambiguity of the term “reasonable” has been labelled problematic in view of modern technological advances.\textsuperscript{123} As PIPEDA’s position on the sensitivity of behavioural data remains undetermined, the reasonability requirement may provide little protection to users’

\begin{flushleft}
\textsuperscript{116} Jones, supra note 28 at para 66.
\textsuperscript{117} PIPEDA, supra note 21.
\textsuperscript{118} Ibid, Schedule 1, s 4.3.2, 6.1.
\textsuperscript{119} Ibid, Schedule 1, s 4.3.2, 6.1; see, e.g. Englander v Telus Communications Inc, 2004 FCA 387 at para 67.
\textsuperscript{120} Ibid, Schedule 1, s 4.3.4; While “medical information is almost always considered to be sensitive, calling for a rather more explicit form of consent,” (Townsend v Sun Life Financial, 2012 FC 550 at para 25) the Federal Court has gone as far as recognizing the sensitivity of data involving the frequency with which an individual visits a fitness center (Randall v Nubody’s Fitness Centres, 2010 FC 681). Essentially, based on the facts of that case, “the information was sensitive particularly as it was being disclosed to [the applicant’s] work colleagues at a staff meeting and encouraged rivalry with colleagues that made him uncomfortable” (Ibid at para 43).
\textsuperscript{121} Office of the Privacy Commissioner of Canada, “Bank does not Obtain the Meaningful Consent of Customers for Disclosure of Personal Information”, “PIPEDA Case Summary #2003-192 (23 July 2003), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-192/> (“(1) The personal information must be demonstrably non-sensitive in nature and context; (2) The information-sharing situation must be limited and well defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure; (3) The organization's purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected; (4) The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of the procedure at the time the personal information is collected.”); See also PIPEDA, supra note 21, Schedule 1, s 4.3.6.
\textsuperscript{123} Dubrovsky, supra note 27 at 177-179.
\end{flushleft}
digital privacy. If this behavioural data is not considered sufficiently sensitive, PIPEDA’s consent requirement may technically be satisfied when obtained with a lack of transparency, yet the consent would be far from meaningful. Should future courts adopt this threshold for consent, the Intrusion and Public Disclosure torts’ application to interconnected environments may be limited.

Tort law’s consent requirements are more stringent than PIPEDA’s, which has led some scholars to contend that the Intrusion and Public Disclosure torts require a higher consent threshold. Essentially, “[the] tort law version of consent doesn’t depend on formalities like opt-in or opt-out. Rather, it requires that the subject appreciate the act that she consents to and be in fact willing that it occur.” Users’ ability to appreciate the “dataveillance” practices they are consenting to is limited for two reasons. First, users generally cannot “accurately assess the magnitude of loss [due to their] inadequate understanding of how much data the profilers can obtain and how the data describes even some of the most intimate details about [them].” Second, while corporate surveillance “occurs because we ostensibly agree to it,” this does not “mean that we make an informed decision agreeing to it; instead, we accept it either because we get value from the service or because we are offered a package deal that includes surveillance and don’t have any real choice in the matter.” The consent acquired by companies to collect and disclose users’ behavioural data is therefore unlikely to satisfy tort law’s threshold.

Regardless of what consent threshold is adopted in regard to the Intrusion and Public Disclosure torts, two factors may still preclude their application to “dataveillance” practices. The first factor arises in the context of the Intrusion tort, the defence of lawfully justified intrusions. Lawful justification is a broader concept than mere authorization, thus excluding a wider range of activities from this tort’s scope. For example, the Privacy Commissioner’s finding that personal information collected and used for behavioural advertising is a necessary corollary to enjoying free websites may be a sufficient “lawful justification” to enable such intrusions irrespective of consent.

124 Ibid.
126 Tran, supra note 45 at 296; Jessica Litman, “Information Privacy/Information Property” (2000) 52 Stan L Rev 1283 at 1310-11 (“What counts or should count as effective consent has been one of the most contentious issues in the privacy debate” at 1310) [Litman].
127 Litman, ibid at 1310-11.
128 Berger, supra note 47 at 24-25.
129 Schneier, supra note 2 at 47.
This approach could limit actions in Intrusion even where users specifically demonstrate their lack of consent or neglect to provide it in the first place.

The second factor arises in the context of the Public Disclosure tort: the publicity criterion is very difficult to meet when it comes to disclosures of behavioural data for advertising purposes. Although not defined in the Doe decision, the American Restatement maintains that “‘publicity,’ as it is used in this Section, […] means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.” American law has interpreted this dissemination requirement “to mean general distribution to the public […] and not just circulation of personal information among a closed group of people.”

There are three common ways that others discover and access the personal data collected in interconnected environments. The first is through disclosure to third-party companies. In addition to being a practice that users generally consent to by accepting corporate privacy policies, this is unlikely to satisfy the disclosure requirement because it is not sufficiently wide dissemination to result in publicity. Moreover, the
data is usually transferred in aggregate form, which the Privacy Commissioner does not consider as constituting “disclosure” under PIPEDA.\(^{137}\) The second way behavioural data is discovered is when hackers gain unauthorized access to this information due to security flaws in corporate systems or personal devices. However, it is unclear whether this “disclosure” is sufficiently public to satisfy the publicity criterion and whether the hacked company can even be held accountable, which Part III will further address.\(^{138}\)

Finally, when devices are shared by different users or used in public, behavioural information can be discovered through the creation of personalized ads within browsers or devices, since online searches for sensitive topics such as sexual orientation, humiliating illnesses, or financial troubles “sometimes lead to related ads appearing on [a user’s] computer screen,”\(^{139}\) or through the sending of unsolicited advertisements based on this information to consumers via email or text message. It is useful to point out that, in the latter case, users may enjoy a higher level of protection than PIPEDA would provide for the misuse of their personal information. In essence, unsolicited electronic messages—colloquially known as spam—are governed by the Canadian Anti-Spam Act, which imposes a stricter consent requirement\(^{141}\) than PIPEDA, only allowing for consent to be implied in very limited situations.\(^{142}\) This demonstrates that “federal law recognizes that consumers have heightened privacy protections related to personal data associated with their mobile phones [and other electronic messaging disclosures have been made. Even if people are generally aware that their data is being transferred, they will often not be able to find out the specifics – what companies are receiving it and what these companies plan to do with it. As a result, the public disclosure tort is not well-adapted to combating the flow of personal information between various companies” at 60); Elbert Lin, “Prioritizing Privacy: A Constitutional Response to the Internet” (2002) 17 Berkeley Tech LJ 1085 (“[the personal information aggregated via interconnected devices] that is widely disseminated may be […] [part of the] public record […] [and] not tortious […] [but] [c]onversely, [the data] that [is] […] seemingly private […] [is] often considered not to have been widely disseminated” at 1091-92); Jamuna D Kelley, “A Computer with a View: Progress, Privacy and Google” (2008) 74 Brook L Rev 187 at 209.

\(^{137}\) CIPPIC, supra note 130 at para 132.
\(^{138}\) See below, p 25.
\(^{140}\) An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying on commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23, s 1, 6(1) [Anti-Spam Act].
\(^{141}\) Ibid, s 10(1), 6(1)
\(^{142}\) Consent can only be implied if (a) there is an existing relationship with the person, (b) the electronic address or mobile number of the person receiving the message is publicly available and did not indicate that they do not wish to receive unsolicited messages, (c) the person receiving the message has disclosed their electronic address or mobile number and did not indicate that they do not wish to receive unsolicited messages, or (d) the circumstances under which the message is sent is set out in applicable regulations (Ibid, s 9).
\(^{143}\) King, supra note 93 at 296-297.
accounts],” and that these individuals may thus enjoy a heightened level of protection for any of their private information that is disclosed through electronic messages.

The potential disclosure that may occur as a result of behavioural advertisements or spam results from sharing devices or using them in public. Therefore, proving a Public Disclosure claim may be difficult in such cases if this conduct is viewed as tacit consent to the advertisements or spam being viewed by others. There are, however, two elements that may favour the opposite conclusion. First, if users did not consent to being targeted with ads or messages based on their sensitive information, they could not have known prior to sharing their devices or using them in public that they may be publicizing such facts about themselves in doing so. Moreover, since the Supreme Court has recognized the right to a certain measure of privacy in public, this could extend privacy protection to individuals using their devices in the presence of others. Second, the simple publication of these ads may be sufficient to engage the Public Disclosure tort in Canada. The American Restatement differentiates between the terms “publicity” and “publication,” stating that the latter merely requires communication to a third person rather than wide dissemination. In contrast, Doe reconceptualised the tort of Public Disclosure to specifically mention the “act of publication.” If this reformulation is interpreted so that the act of publication is sufficient to engage the tort of Public Disclosure, the creation of personalized ads in browsers or devices may be actionable. The remaining criteria, however, must still be satisfied. Whether or not these ads would be considered to engage sufficiently private facts so as to be considered “highly offensive,” for example, remains unclear.

Even if the publication of a personalized ad could engage the tort of Public Disclosure, two critical issues remain. These issues involve freely available applications that block ads on browsers and devices, which could affect the validity of Public Disclosure claims. First, a claim may be unavailable to users who could avoid such “publicity” through the installation of ad filtering software, but fail to do so. Taking such positive steps towards personal information protection has been considered by some American courts as favourable to recognizing privacy in public spaces.

However others have argued that recovery should not be barred merely because the

---

144 Aubry, supra note 108.
146 Doe, supra note 34 at para 46.
147 See e.g. AdBlock Plus, online: <www.adblockplus.org/>; Ryan Whitwam, “New ‘Perceptual Ad Blocker’ may be impossible for websites to defeat”, ExtremeTech (17 April 2017), online: <www.extremetech.com/internet/247808-new-perceptual-ad-blocker-may-impossible-websites-defeat>.
149 See Gines-Perez, supra note 94 at 225; Konop, supra note 94 at 884; Yath, supra note 94 at 51 (Johnson J, concurring); Pietrylo, supra note 94 at *2; see also Pabarcus, supra note 20 at 423.
consumer could have prevented any invasion by using an opt-out mechanism. 150 Second, a claim may be unavailable to a person if they do install an ad filter but disable it to access certain websites. While deactivation may imply authorization to publish the ads on those websites, the growing number of websites requesting or requiring that ad blocking software be disabled casts doubt on this proposition. 151 Regardless of the reasonableness of this position, there are several factors that may prevent targeted personalized ads from being viewed as “publicity” (or “publication”).

This section has raised several uncertainties that may affect the application of the Intrusion and Public Disclosure torts to instances of “dataveillance.” While the Intrusion tort’s application may be limited for any lawfully justified purpose, proof of wide dissemination required by the Public Disclosure tort appears even more prohibitive. Nevertheless, an action in privacy torts may be available for the collection and disclosure of sensitive data, because there is little that could justify the use and dissemination of such information without consent. Whether a possibility of pursuit exists for similar uses of other behavioural data remains to be seen.

Highly Offensive to a Reasonable Person: Does Anything Still Shock Us in The Information Age?

The torts of Intrusion and Public Disclosure require the conduct complained of to rise to the level of “highly offensive.” In Intrusion, the intrusion at the heart of the claim must be highly offensive to the reasonable person, whereas in Public Disclosure the private facts publicized, or the act of publication, must be highly offensive to a reasonable person. Many have contended that the obligation to prove that an invasion is “highly offensive to the reasonable person” may unduly limit the scope of Intrusion in a world where heightened surveillance has detrimentally lowered reasonable expectations of privacy. 152 Essentially, “the oftentimes overwhelming encroachments on privacy that are increasingly […] visited on persons in the age of technology [have] served to desensitize us to their unreasonableness [and have] accordingly come to gain tacit

150 McKinney & Whitten, supra note 77 at 767.
152 See Reidenberg, supra note 134 at 223 (“[i]n the context of data processing activities, an invasion of this right can only result from the techniques used to collect personal information… [and] the particular means used to collect personal information must be highly offensive…Surreptitious or secret collections of personal information without notice or consent may be considered harmful by individuals, yet not rise to a sufficiently ‘objectionable’ level to meet the threshold standard” at 223).
acceptance in some contexts.” Due to society’s growing acquiescence to corporate “dataveillance,” “the expectation-focused standard, centering on the perceived reasonableness of the invasion of privacy, [may render] even the most manifest intrusions presumably inactionable in tort.”

While many digital intrusions will not be actionable in tort, there are certain situations that seem to satisfy the “highly offensive” criterion. One example concerns the locations where mobile phone users are tracked. This intrusion is more likely to be viewed as “sufficiently sensitive and intimate in that it would allow [mobile advertisers] to track consumers’ activity from place to place—tracking that may perhaps be viewed by consumers as ‘commercial stalking’ […] [and thus as transgressing] the kinds of social norms whose violation would properly be viewed with outrage or affront.” Therefore, the “highly offensive” requirement may not bar all modern-day technological intrusions.

Similarly, the “highly offensive” criterion in Public Disclosure may limit the tort’s ambit, since “online conduct has had a disinhibiting effect over time, and has desensitized us to offensive content.” However, some data collected through interconnected devices is likely to remain highly offensive to the reasonable person, such as sexual practices, financial details, or health information. This data is offensive not only due to its content, but also because of the “heightened potential for abuse.” For instance, financial details are rife with potential for financial fraud. Health information could easily become an embarrassment, and might, in an extreme case, even hamper the consumer’s ability to get employment or insurance.

Therefore, the facts or publication of such facts may also be highly offensive due to the potential for their disclosure to lead to discrimination.

154 Ibid at 203; See also Hunt, supra note 88 (discussing how “attaching the [highly offensive] qualifier not only undermines the basis for the action – that it is an affront to one’s dignity – but that it is redundant in light of a reasonable expectations-based test” at 689).
155 See e.g. Berger, supra note 47 (“the requirement that the intrusion be ‘highly offensive to a reasonable person’ establishes a high threshold for liability. It is not clear, for instance, that when AOL recorded that Ms. Arnold searched for men near her age [and her identity was discovered and published in the newspaper along with the search terms she used], the intrusion would be highly offensive to a reasonable person, particularly if one purpose of the “intrusion” was to allow AOL to satisfy Ms. Arnold’s search request” at 35).
156 King, supra note 93 at 296; See also Robert C Post, “The Social Foundations of Privacy: Community and Self in the Common Law Tort” (1989) 77:5 Cal L Rev 957 at 962.
157 Lipton, supra note 47 at 150-151.
158 Jones, supra note 28 at para 72; McKinney & Whitten, supra note 77 at 773.
159 Berger, supra note 47 at 25-26.
160 Tran, supra note 45 at 288.
Even if the offensiveness of intrusions or facts is established, the “highly offensive” factor may still lead to failed claims in Intrusion or Public Disclosure on one additional basis:

[these torts] can only apply to specific collection of one user’s information through one instance of [behavioural targeting], [and] it is improbable that the finder of fact would find a singular disclosure under either to pass such a strict standard. Indeed, the collection or disclosure of user information through [behavioural targeting] might only pass the standard when considered in the aggregate as a large-scale intrusion upon the privacy rights of ‘hundreds of actors over a long period of time’ [which] conflicts with the limited remedies afforded by the common law tort system.161

Nevertheless, some contend that this view is unfounded considering consumers’ option to institute privacy class action lawsuits.162 The recent certification of several such pursuits by Canadian courts in cases involving access to sensitive personal information resulting from offensive breaches seems to favour the latter position.163 Whether or not such class actions will be permitted to go forth for privacy violations arising from corporate “dataveillance,” however, remains to be seen.

Concluding Remarks: The Future of Privacy Torts’ Application to Corporate “Dataveillance”

There are several variables that could affect the application of the Intrusion and Public Disclosure torts to corporate “dataveillance” practices. The scope of each tort will depend on future courts’ interpretation of the following criteria: (1) whether “private affairs or concerns” and “private facts” are considered to encompass all personally identifiable information or merely sensitive data, (2) whether the required consent threshold will render user authorizations acquired by corporations to mine and disclose behavioural data inadequate, and (3) under what circumstances the “highly offensive” criterion will be met. For each tort to extend to instances of digital privacy violations, the following interpretations will likely be necessary: “private affairs or

---

concerns” and “private facts” must encompass more than highly sensitive data; the consent threshold must be high enough to render the often implicit user authorizations acquired by corporations inadequate; and the “highly offensive” criterion will have to be interpreted flexibly, given that modern society is largely desensitized to offensive material. Furthermore, the applicability of Intrusion will require a restrictive interpretation of “lawful justification,” and the applicability of Public Disclosure will require a broad interpretation of “publicity.” Clearly, there are several undecided issues that contribute to an uncertain future for the intersection of tort and digital privacy.

The uncertainties arising from this analysis are a double-edged sword. While it is difficult to predict whether the privacy violations associated with the Internet of Things will be actionable in either Intrusion or Public Disclosure, the recognition of these torts will not “open the floodgates” in a manner that would negatively impact the economic stability of electronic commerce and web-based companies. Despite these reservations, it may be possible to hold companies liable in tort for privacy breaches suffered by users at the hands of hackers.

III. MALICIOUS USERS VS. PRIVATE COMPANIES: WHO SHOULD BE HELD LIABLE FOR PRIVACY VIOLATIONS SUFFERED BY INNOCENT USERS AT THE HANDS OF HACKERS?

Due to the relative novelty of Intrusion and Public Disclosure in Canada, some parts of the legal community are attempting to see how wide protection can span with respect to informational privacy. A number of class action lawsuits have recently been instituted alleging privacy invasions for the loss, misuse, or unauthorized access of personal data by hackers or other private entities. The results of many of these cases, either having been dismissed or settled outside of court “indicate that both class counsel and Canadian courts recognize the difficulties inherent in proving damages from data breaches. The cases are also indicative of the litigation risks companies face even when data breaches are caused by third parties’ actions.” Although several recent data breaches by hackers have resulted in consumers rallying to pursue the

164 Jones, supra note 28 at para 72.
165 Condon, supra note 163 (certifying class action lawsuit).
166 Hopkins, supra note 163 (certifying class action); Evans, supra note 163 (finding that it is not plain and obvious that a bank cannot be held vicariously liable for breaches to privacy committed by its employees).
167 Lozanski, supra note 163 (settled); Lenovo, supra note 163.
168 Lozanski, ibid (Although this case did imply that actual harm suffered would have to be proven in such cases, the Ontario Court of Appeal’s decision in Jones v Tsige specifically permits moral damages even where no economic harm was suffered and it is the latter decision that will take precedence in cases applying the Intrusion tort).
169 Ibid; Lenovo, supra note 163.
170 Talbot, supra note 71 at 41.
affected companies for unauthorized access of their personal information, only one such case has so far been heard by the courts. This case was unfortunately settled without further assessing the applicability of privacy torts to such situations. While privacy torts may be applied to similar situations in the future, this approach is not without its obstacles. The success of such a claim would be dependent on a certain legal imagination, similar to the approach adopted in Jones. 

There is no doubt that the unauthorized access of hackers to corporate databases and user devices is actionable in tort. Unfortunately, malicious users are so adept at covering their tracks that they can be impossible to locate for legal pursuit. Consequently, it has been questioned whether the hacked corporations could be held liable for these violations, because the breaches generally result from security flaws in their systems or in the devices they distribute to users. While many argue that the Intrusion and Public Disclosure torts’ formulation make it impossible to hold an individual liable who did not directly initiate the actionable intrusion or disclosure, or that a new tort is necessary to govern such situations, this perceived gap in the law may be addressed by a creative application of Intrusion and Public Disclosure.

Assuming that the affairs, concerns, or facts accessed by the hackers are sufficiently private to engage Intrusion or Public Disclosure, and that the personal data of ordinary citizens is unlikely to be of legitimate public interest, we will address the remaining elements necessary to establish these torts. Whereas the tort of Intrusion requires the defendant to have invaded a person’s private affairs, the tort of Public Disclosure requires that the defendant give publicity to a private fact. While this implies

---

172 Lozanski, supra note 163.
175 See Borzykowski, supra note 72.
176 Lipton, supra note 47 at 930; Vodovis, supra note 44 at 818.
177 Vodovis, supra note 44 at 831-832; Lessig, supra note 72 at 515.
necessity for the defendant to have directly accomplished these actions to be liable for them, where such an occurrence takes place due to the recklessness or intention that may be imputed to another entity, it may be possible to establish the Intrusion and Public Disclosure torts respectively.

The *Jones* decision provided very little guidance regarding the recklessness standard’s application to the Intrusion tort; however, the term is generally conceptualized as having “both a subjective component (awareness that one is creating a serious and relatively easily avoidable risk of harm to others) and an objective component (one’s conduct, assessed objectively, must be negligent),”¹⁸⁰ where the defendant reasonably ought to have foreseen the risk. This standard may therefore be very difficult to prove in the context of interconnected technologies, where the risks are infinite and potentially unforeseeable.

Imputing the intention of hacked corporations regarding the consequences suffered as a result of a data breach may be equally difficult. The possibility, however, may exist under some circumstances to the extent that “conduct is also intentional if the consequences, while not desired, are substantially certain to result from the defendant’s conduct.”¹⁸¹ While this standard would not make it possible to pursue a corporation for all breaches to their systems by hackers, there are two instances that have potential to satisfy the standard. The first is where companies do not at least conform to accepted cybersecurity industry standards. Enabling hacking by neglecting to meet industry accepted security standards such that systems are riddled with vulnerabilities is sufficiently serious to warrant the same consequences as intentional hacking. The fact that the company is not the one actively intruding on users’ personal data should not be used to deny legal recourse to victims of such breaches. It is precisely this type of legal imagination that was implemented in *Jones* to provide redress for a privacy violation that simply “[cried] out for a remedy.”¹⁸² The invasions suffered by victims of hackers is another such situation.

The second instance whereby a company’s conduct might be construed as intentional is when it neglects to notify its users of a known breach to allow for preventative actions to be taken against future intrusions.¹⁸³ Although this intentional conduct is not the cause of the initial intrusion, it will likely be responsible for any future intrusions that are substantially certain to occur if users’ private information is misused by hackers. The substantial certainty that harm may be suffered, where users are not notified of a breach to their personal information, can be illustrated by the recent multiple hackings of Yahoo’s system, which compromised the private information of

---

¹⁸² *Jones*, *supra* note 28 at para 69.
¹⁸³ Talbot, *supra* note 71 at 41.
one billion users. In this case, Yahoo only publicized the breach three years after its occurrence, and “due to the lack of proper notification and security measures taken by Yahoo, several victims have suffered substantial financial burdens.”\textsuperscript{184} One user implicated in this breach was “unable to file his tax return because a return had already been filed under his Social Security number, which led to numerous fraudulent charges on his credit cards plus $9,000 in college expenses for his daughters who were unable to apply for financial aid on time.”\textsuperscript{185} Another user affected by this hack had her Social Security benefits stolen as a result of her compromised email account.\textsuperscript{186} Although Yahoo claimed that it was difficult to tie the breaches to the harms suffered, its position was rejected by the United States District Court, which allowed the class action lawsuit to proceed.\textsuperscript{187}

While users who did not suffer actual harm have often been met with obstacles when attempting to argue that they are at risk of future identity theft, those who have suffered an avoidable harm due to the company’s failure to notify them of the breach might be successful in demonstrating an element of intention on the corporation’s part. Although the Canadian courts have not yet encountered such a case, this position appears to be in line with recent amendments made to PIPEDA. The recent amendments require mandatory breach notifications where there is a “real risk of significant harm,”\textsuperscript{188} such as where social insurance numbers are surreptitiously accessed. Inasmuch as this risk can be mitigated by merely notifying users, one might even venture to say that companies neglecting to do so are behaving recklessly. Essentially, they are aware that they are creating a risk that might promptly be moderated by users if they were otherwise informed. Such conduct is, objectively speaking, negligent.

The possibility of demonstrating that a hacked corporation acted with intent or recklessness in the above circumstances, however, may only be sufficient to engage the Intrusion tort rather than the Public Disclosure tort. The former only requires an intrusion into private information to have occurred, whereas the latter further necessitates wide dissemination of the private fact. Although this element is unlikely to be established in a claim of Public Disclosure against a hacked company,\textsuperscript{189} it will depend on the facts of the case. For example, a system infiltrated by a large group of


\textsuperscript{186} \textit{Ibid}.

\textsuperscript{187} \textit{Ibid}.


\textsuperscript{189} Vranas-Liveris, supra note 178 at 666.
hackers is more likely to favour this criterion than one accessed by a single malicious user. Cases where the data obtained is released into the public sphere, such as the infamous Ashley Madison hacks,\(^\text{190}\) are most likely to satisfy this criterion.

The “highly offensive” criterion is also easier to establish for Intrusion than for Public Disclosure. The former tort requires the intrusion itself to be offensive. Despite society’s general desensitization to privacy violations in the digital era, people remain highly offended when malicious users hack into personal devices or corporate databases,\(^\text{191}\) and they are just as affronted when corporate security measures fail to prevent such breaches.\(^\text{192}\) However, with Public Disclosure necessitating that the private fact disclosed or the act of publication be “highly offensive,” this tort may only be engaged in limited situations where the hacked data is highly sensitive, as discussed above.

There is therefore a possibility to recognize corporate liability in Intrusion, if not in Public Disclosure, for breaches to corporate databases by hackers under some circumstances—especially where users are not notified in a timely manner that their data has been compromised. This approach is currently being tested by lawyers instituting class action lawsuits against Equifax and Yahoo due to major breaches of their systems by hackers that implicated the private information of thousands of users.\(^\text{193}\) Whether or not they will be successful remains to be seen. Not all is lost, however, in cases where all the privacy torts’ elements cannot be established in the face of such security breaches. Users may still be able to claim monetary redress by instituting actions in virtue of breach of contract or negligence. The former would be premised on the corporation’s failure to safeguard their personal information as stipulated in the agreement between the business and consumer,\(^\text{194}\) and the latter would assert that they neglected to institute industry accepted security standards.\(^\text{195}\)

\(^{190}\) Kim Zetter, “Hackers Finally Post Stolen Ashley Madison Data” (18 August 2015), Wired, online <www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data>.


\(^{192}\) Ibid.


IV. PRIVACY, FREEDOM OF EXPRESSION AND FREE FLOW OF INFORMATION VS. STABILITY OF THE DIGITAL ECONOMY: HOW CAN ONTARIO PRIVACY LAW EVOLVE TO ADDRESS THE INTERNET OF THINGS?

While the “public’s right to [the free flow of] information, supported by freedom of expression, [generally places] limits on the right to respect for one’s private life in certain circumstances…[where] the expectation of privacy is reduced,”\(^\text{196}\) the opposite position holds true with respect to users subjected to “dataveillance.” In interconnected environments, embracing the values of freedom of expression inherently means embracing those of privacy. The ability to view online content anonymously, without being subjected to the possibility of identification by corporate entities, the government, other users, or the general public, is crucial to ensure that Internet users are not self-censored or inhibited\(^\text{197}\) such that they feel free to access all data without fear of surveillance—information that they may later use as a basis for legitimate expression.\(^\text{198}\) Protecting the freedom of expression and the free flow of information is thus intrinsically linked to safeguarding privacy in digital arenas.

Although upholding these important values may support increased privacy protection, doing so may upset the economic stability of these spheres by placing too much liability on web-based companies providing free commercial services. With users refusing to pay for these services in traditional currency, the use of their personal data for advertising is the necessary corollary to sustaining the Internet’s current business model.\(^\text{199}\) In the context of Facebook, for example, the Privacy Commissioner has “[acknowledged] that Facebook needs to have a means of generating revenue and most Facebook users reasonably expect to receive advertisements. In the circumstances of Facebook’s ostensibly ‘free’ social networking service, [the Privacy Commissioner finds] it reasonable that users are required to consent to Facebook Ads as a condition of service.”\(^\text{200}\)

---

\(^{196}\) Mackey, *supra* note 26 at 12.


\(^{198}\) Niva Elkin-Koren, “After Twenty Years: Revisiting Copyright Liability of Online Intermediaries” in Susy Frankel & Daniel Gervais eds, *The Evolution and Equilibrium of Copyright in the Digital Age* (Cambridge: Cambridge University Press, 2014) at 44-45; see also Pabarcus, *supra* note 20 (“To adequately address the problems of privacy on the Internet, the law should enforce an individual’s social expectations of confidentiality. Such expectations should be enforced even if surveillance is covert and the victim is never aware of the actual intrusion, because the harms have a chilling effect on behavior and speech on the Internet through intrusion.” at 410); Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 191.

\(^{199}\) Schneier, *supra* note 2 at 50; Robison, *supra* note 130 (“a customer’s privacy is the true cost of “free” [online] services” at 1214); CIPPIC, *supra* note 130 at para 134.

\(^{200}\) CIPPIC, *supra* note 130 at para 134.
Granting that it would be unwise to “open the floodgates” of Intrusion and Public Disclosure actions to minor digital privacy violations, it is unlikely that providing corporations with incentive to better protect user privacy would upset the balance of e-commerce. The veracity of this statement can be demonstrated by the success of the privacy protection regime established in the Province of Quebec, whose legislation provides for a blanket allowance to sue for breaches to informational privacy. Despite this, the floodgates of such pursuits have not opened—with only 75 complaints having been received over the 2015–2016 period, as discussed in the last yearly report issued by the Commission de l’accès à l’information responsible for investigating such claims. Moreover, rather than hindering the economic stability of business in this province, Quebec’s digital economy has seen a great resurgence in recent years with a number of high-profile companies creating cloud computing data centers—which both store and process infinite amounts of private user data—on Quebec’s territory.

Therefore, the suggestion of this paper is that the legislature modify certain PIPEDA provisions and that the judiciary work towards a clear definition of the key elements of invasion of privacy torts to ensure the ability to apply these torts to corporate “dataveillance” practices and privacy breaches by hackers. To begin, considering the contention in Jones that privacy torts protect informational privacy interests, there are two appropriate modifications to be made in PIPEDA. First, a clear threshold should be established to simplify the distinction between data that is merely “personally identifiable” and that which is truly “private” or “sensitive.” The lack of precision surrounding the types of data that can truly be considered “private” makes it difficult to determine whether or not they are actionable privacy torts. For example, is a company’s collection of “real-time digital notes on how [customers] responded to [their vibrator’s] ‘pulse’ mode compared to ‘cha cha’” actionable as pertaining to “sexual practise” or would the law view it as something less? Is a snippet of a person’s conversation recorded against their wishes by their Smart Home device an actionable private correspondence, or will this depend on whether the words spoken contain “private” details?

---

201 Their legislation allows for the civil pursuit of any company that (1) commits a privacy violation that runs contrary to their legislative equivalent of the PIPEDA (See Eltis, supra note 153; See also Mizrahi, supra note 50) and (2) that violates the privacy provisions of the Quebec Charter of Rights and Freedoms (See Aubry, supra note 108).


204 Jones, supra note 28 at para 66.

205 Brownwell, supra note 56.

206 Maheshwari, supra note 60.
Second, PIPEDA should be modified to clearly enunciate what qualifies as reasonable consent in various circumstances. The reasonability element is largely illusory when applied to interconnected environments because “[it] is not effective in protecting a user’s right to online privacy as technological advances create circumstances that go beyond the reasonable person’s considerations and expectations. Most Internet users may not understand the types of threats presented online or the types of technologies available.” This difficulty can be avoided by requiring express consent to corporate “dataveillance” practices. This approach would “[remove] the ambiguity underlying the role of consent [thus placing users] in a better position to ensure that they are not implicitly agreeing to a use that they otherwise would not consent to and [allowing] businesses [to] better protect themselves from potential complaints based on making a wrong discretionary choice.”

In regard to the interpretation of the Intrusion and Public Disclosure torts’ elements, this paper also makes a significant recommendation. The scope of the “highly offensive” criterion should be clarified. Despite the few above-outlined examples likely to satisfy this criterion, society’s desensitization to “dataveillance” practices may bar action to some truly offensive intrusions or disclosures. To avoid unnecessarily limiting the Intrusion and Public Disclosure torts’ application, a contextual approach, like the English subjective-objective test, would be appropriate to determine the actionability of privacy invasions. This test inquires “whether there is a reasonable expectation of privacy. This is of course an objective question […] [But] the reasonable expectation [is] that of the person who is affected by the [intrusion or] publicity […] ‘The question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same [intrusion or] publicity.’” This flexible approach considers all relevant circumstances, making it “inherently well suited to respond to unforeseen privacy threats arising from technological and social changes, which have obvious impacts on the analysis of legal privacy rights.”

---

207 Dubrovsky, supra note 27 at 177-179.
208 Ibid at 177.
209 Ibid at 178-179.
211 Murray v Big Pictures (UK) Ltd, [2008] EWCA Civ 446 at para 35 [Murray].
212 Ibid (the relevant circumstances include: “[1] the attributes of the claimant, [2] the nature of the activity in which the claimant was engaged, [3] the place at which it was happening, [4] the nature and purposes of the intrusion, [5] the absence of consent and whether it was known or could be inferred, [6] the effect on the claimant [7] the circumstances in which and [8] the purposes for which the information came into the hands of the publisher” at para 36).
protection, while the assessment of societal norms ensures that this will not lead to absurd results. Moreover, the test’s contextual approach to a claim’s reasonableness “reflects [its] relativistic premise – that privacy is a ‘matter of fact and degree rather than a matter of absolutes’ and it thereby avoids the problems of categorization and bifurcation identified above.”

In addition to the above-noted clarifications, the courts should be willing to treat a company’s decision to utilize inadequate security measures as sufficient to engage the torts of Intrusion and Public Disclosure where the risk to privacy is appreciated, as discussed above. The ability to hold corporations accountable for such privacy breaches will have to be premised on a high standard of recklessness to prevent imposing impossible security standards on these entities. Only the most inadequate cybersecurity levels should ground liability in these torts, such as where companies fail to conform to accepted industry standards or fail to make improvements despite facing repeated hacking attacks. There are already encouraging signs that our legal system is willing to recognize the role of corporations in mitigating the threats imposed by hackers, such as the imposition of an obligation for corporations to disclose privacy breaches under PIPEDA.

CONCLUSION

The digital economy endows users with very little power. While it is essentially impossible to be an active member of society without using interconnected devices, this reality leaves individuals with no choice but to accept corporate “dataveillance” practices. Furthermore, users are largely deprived of control in securing their informational privacy. They are vulnerable in the fight against unauthorized access to their personal data and, despite these significant threats, legal recourse remains minimal.

In the absence of modifications to PIPEDA that would permit the Privacy Commissioner to provide users with monetary redress—which would perhaps be the ideal solution under the circumstances—the compensatory nature of tort law can provide a solution to the predicament users find themselves in. Nevertheless, the privacy torts meant to achieve this feat are riddled with uncertainties in their application and leave much to be desired. With the ambiguity surrounding the Intrusion and Public Disclosure torts’ extension to modern “dataveillance” practices and systematic breaches


215 Hunt, supra note 88 at 687-689.

by unauthorized intruders, these torts have a long way to go in providing adequate protection to digital privacy as a societal value. Although consumers may still have a case under breach of contract or negligence, their ability to gain compensation under either invasion of privacy tort might become increasingly difficult. This challenge results from the upper hand corporations hold in negotiating power, which often forces consumers to agree to terms that may be disadvantageous and serve to prevent them from instituting such claims against companies.

Despite the possibilities for the law to provide digital privacy protections, the rapid progression of technology coupled with the slowly evolving nature of the common law, ensures that the latter will always be behind. The common law, therefore, will always serve as a reactive solution rather than a proactive one and may be insufficient on its own to address these issues. Legislation, however, offers a more proactive solution, which is why there is hope that PIPEDA will be amended to allow for the possibility of compensating users whose privacy is violated by companies and hackers alike. Until changes are instituted in legislation, however, the numerous pending cases instituting privacy tort claims that have been certified by Canadian courts lead to hope that the urgent need for privacy protections will be recognized and addressed within the common law.