

Electronic Thesis and Dissertation Repository

10-12-2017 12:30 PM

Implementing Canada's Data Exclusivity Obligations and Protecting Personal Information in Clinical Trials

Alison Wong, *The University of Western Ontario*

Supervisor: Margaret Ann Wilkinson, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Laws degree in Law

© Alison Wong 2017

Follow this and additional works at: <https://ir.lib.uwo.ca/etd>



Part of the [Law Commons](#)

Recommended Citation

Wong, Alison, "Implementing Canada's Data Exclusivity Obligations and Protecting Personal Information in Clinical Trials" (2017). *Electronic Thesis and Dissertation Repository*. 4969.
<https://ir.lib.uwo.ca/etd/4969>

This Dissertation/Thesis is brought to you for free and open access by Scholarship@Western. It has been accepted for inclusion in Electronic Thesis and Dissertation Repository by an authorized administrator of Scholarship@Western. For more information, please contact wlsadmin@uwo.ca.

ABSTRACT AND KEY WORDS

This thesis explores, in the context of pharmaceutical clinical trials, Canadian federal, provincial and territorial personal data protection laws (which are consistent with Canada's membership in the international Organization for Economic Cooperation and Development). This thesis establishes that, despite scholarly concerns over de-identifiability of data, these laws govern collection, use, dissemination, and disposal of data about individuals in clinical trials right through and including applications made by innovator pharmaceutical companies to the federal government for approval to market new drugs. At this latter point, federal data exclusivity regulations also apply (as required by international trade agreements). This thesis establishes that both personal data protection and data exclusivity apply to clinical trials only for defined periods. Finally, this research demonstrates that, unlike protection of confidential information which remains secret and does not contribute to the public good of access to information, data exclusivity displays characteristics of classic intellectual property.

Key words: data exclusivity, personal information, personal data protection, personal health information, clinical trials, data identifiability, confidential information, intellectual property

ACKNOWLEDGMENTS

First, I thank my thesis supervisor, Dr. Margaret Ann Wilkinson, from the University of Western Ontario, for her expertise, support, and guidance during the research and writing of my thesis and throughout my LLM program.

I also thank the second reader of my thesis, Professor Chios Carmody, from the University of Western Ontario, for reviewing my work and providing insightful comments.

I also thank Mary Morris, graduate programs coordinator, from the University of Western Ontario, for her administrative support on numerous occasions during the preparation of my thesis and throughout the academic term.

I also thank my Thesis Examination Committee, Professors Chios Carmody, Michael Coyle, and Ava John-Baptiste, all from the University of Western Ontario, for reviewing my thesis, conducting my thesis defence, and providing helpful suggestions.

I also thank Professors Margaret Ann Wilkinson, Samuel Trosow, and Gillian Demeyere for their guidance in courses taken during my LLM program.

I am grateful to the librarians, John Sadler and Elizabeth Bruton, and the library assistant, Duncan Archibald, from the John & Dotsa Bitove Family Law Library, University of Western Ontario, for their research assistance during the preparation of my thesis.

Finally, I thank my parents, Rosalind Wong and Bing-Sun Wong, and my sister, Anna Wong, for their continuous encouragement and support during my law studies.

Table of Contents

ABSTRACT AND KEY WORDS	i
ACKNOWLEDGMENTS	ii
List of Tables	vi
List of Figures	vi
Introduction.....	1
Chapter 1 – Historical Background of Constructs	6
1.1. Historical Overview of Drug Regulation	6
1.2. The Movement of Innovation (and Confidential Information) into International Trade.....	13
1.3. Data Exclusivity: Relationship to Intellectual Property and Confidential Information.....	18
1.4. Personal Data Protection: Historical Overview	21
1.5. Personal Data Protection: Questions of Identifiability and Relationship to Data Exclusivity.....	24
1.6. Conclusion.....	25
Chapter Two – Theoretical Background of Constructs	28
2.1 Introduction	28
2.1.1. The Nature of Confidential Information: Excluding Others - The Importance of Confidential Information to Private Businesses.....	29
2.1.2. The Nature of Confidential Information: A Question of Duty	30
2.1.3. The Nature of Confidential Information: The Duty of Confidence in English Case Law	31
2.1.4. The Nature of Confidential Information: The Protection of Confidential Information in Canadian Case Law	34
2.1.5. The Nature of Confidential Information: Questions of Balance - The “Bargain” in Intellectual Property Rights Protection	41
2.1.6. The Nature of Confidential Information: Confidential Information as (Intellectual) Property - Is the Bargain Present?	45
2.1.7. The Nature of Confidential Information: Controlling Confidential Information - The Tension between Access and Secrecy.....	50
2.1.8 The Nature of Confidential Information: Confidential Information is a Wider Class of Information than Trade Secrets	53

2.1.9. Conclusion on the Nature of Confidential Information.....	59
2.2. Regulation of the Drug Approval Process: Protecting Public Health	60
2.3. Access and Control over Confidential Information in the Pharmaceutical Context	65
2.4. Data Exclusivity and Control over Confidential Information.....	75
2.4.1. Pharmaceutical Innovation and Intellectual Property Protection: Safeguarding Investment	75
2.4.2. Nature of Data Exclusivity: Interpretative Context and International Trade ..	80
2.4.3. Nature of Data Exclusivity: Perspective of Proponents – Protecting Public Health and Preventing Free-Riding	83
2.4.4. Nature of Data Exclusivity: Perspective of Opponents – Impeding Public Health while Providing “Double Protection”	85
2.4.5. Nature of Data Exclusivity: Conclusion.....	93
2.5. Uniting the Constructs: Confidential Information, Data Exclusivity, and Personal Data Protection in the Context of Clinical Trials.....	94
2.5.1. Personal Data Protection and the Individual’s Right to Control Information .	95
2.5.2. The Right to Control One’s Personal Information: The Importance of Consent	99
2.5.3. Personal Information Protection: A Matter of Control and Not Ownership .	101
2.6. Conclusion.....	105
Chapter 3 – Data Exclusivity and Personal Data Protection in Canada	107
3.1 Data Exclusivity in Canadian Legislation.....	107
3.1.1. Implementing Data Exclusivity into Canadian Legislation: Judicial Interpretation of the First Regulation	108
3.1.2. Strengthening Data Exclusivity in Canada: The Data Protection Regulation	112
3.1.3. Judicial Interpretation of the Data Protection Regulation in Canadian Case Law	115
3.2. Personal Health Information Legislation: Controlling Information in the Health Context	124
3.3. Linking Data Exclusivity to Personal Data Protection.....	129
3.3.1. Record-Keeping Requirements: Good Clinical Practices and Identification of Patients.....	132
3.3.2. Which Personal Data Protection Laws Apply to Qualified Investigators and Clinical Trial Sponsors?	140

3.4. What Information Qualifies as “Personal Health Information” under Canadian Legislation?	149
3.4.1. The Notion of Identifiability.....	149
3.4.2. Identifiability of the Individual: Application of Personal Data Protection and Control over Information.....	153
3.4.3. De-Identified Health Information: Definitions and Consequences of this Classification	158
3.4.4. Contemplating Technological Realities: Personal Health Information Statutes, Data Matching, and Re-Identification of the Individual.....	165
3.4.5. De-Identification and Re-Identification: Is Data Ever Truly Anonymous? ..	169
3.4.6. Withdrawal of Consent to Use and Disclosure of Personal Information: A Potential Conflict with Data Exclusivity?	171
3.5. Conclusion.....	175
Chapter 4 – Conclusions and Suggestions for Future Research	177
4.1. Conclusions	177
4.2. Future Research.....	184
Bibliography	187
Appendix 1: Summary of Major Findings with Respect to Personal Health Information Protection Legislation	200
Appendix 2: Information Constructs Summary	201
Appendix 3: List of Acronyms	202
Academic CV	203

List of Tables

Table 1 - Jurisdictions with Health-Specific Personal Information Protection Legislation	127
Table 2 - Personal Data Protection Law Applicable Where Jurisdiction Has No Health-Specific Statute	128
Table 3 - Required Records to be kept in the Course of Clinical Trials that can Identify Clinical Trial Subjects.....	134
Table 4 - Application of Health-Specific Personal Data Protection in Clinical Trials...	147
Table 5 - Application of Personal Data Protection in Clinical Trials for Jurisdictions without Health-Sector-Specific Statutes	148

List of Figures

Figure 1 - Flow of Information in the Patent Process	42
Figure 2 - Relationship between Confidential Information and Public Knowledge - Two Solitudes.....	47
Figure 3 - Flow of Information when Access Request is made	52
Figure 4 - Flow of Information with respect to Data Submitted by Merck	68
Figure 5 - Flow of Information with respect to Clinical Trial Data and Patient Data	138
Figure 6 - Flow of Information in a Clinical Trial from a Personal Data Protection Perspective	174

Introduction

Modern intellectual property law seeks to maintain a balance between the rights of individual innovators, the private interests of corporations that dominate intellectual property ownership in many contexts, and the public good in accessing knowledge that will further human progress and development.¹ The development of new pharmaceutical products is an essential endeavor that improves and saves human lives. Pharmaceutical companies invest significant resources into the research and development of new drugs, and the effects of these drugs on human health are evaluated in research studies called clinical trials. The information that is obtained during the course of these clinical trials is valuable to both pharmaceutical companies and the public alike, albeit in different ways. On one hand, pharmaceutical companies consider clinical trial data to be valuable confidential business information, which is subject to intellectual property protections. In contrast, the public interest lies in accessing this information in order to increase the availability of affordable medicines and to advance scientific understanding of the effects of certain drugs on human health. The tension that arises between the interests of pharmaceutical companies and those of the public at large illustrates the reality that there can be different, yet compelling, claims to control over the same set of information.

The need for balance among multiple, potentially divergent interests raises important questions with respect to access and control over confidential information, and specifically over clinical trial data. Since international trade agreements confer

¹ For example, Wilkinson observes that modern copyright law seeks a balance between the interests of the following groups: a) the individuals whose cognitive activity produces innovation; b) the corporations that currently dominate ownership of technologies and influence upon economies; and c) the public. See Margaret Ann Wilkinson, “International Copyright: *Marrakesh* and the Future of Users’ Rights Exceptions” in Mark Perry, ed, *Global Governance of Intellectual Property in the 21st Century* (Switzerland: Springer International Publishing, 2016) 107 at 114-115 [Wilkinson, “Marrakesh”].

temporary, exclusive rights upon pharmaceutical companies to the test data involved in their pharmaceutical products, how do these rights affect public health? In particular, do these rights, known as “data exclusivity” protection, either promote or hinder positive public health outcomes? Moreover, members of the public are entitled to protection of their personal information in both the public and private sectors, in accordance with Canadian personal data protection statutes. These personal data protection rights also extend to the health context, where clinical trials comprise part of the treatment options that are sometimes made available to individual patients. Individual patients access clinical trials under the care of a medical professional and have personal data protection rights in their information under personal health information protection statutes.

The work presented in this thesis arose out of a program of research, which was foreshadowed by my supervisor, Professor Margaret Ann Wilkinson in 2014.² In 2016, she and Professor Mistrale Goudreau, of the Faculty of Civil Law at the University of Ottawa, obtained a grant from the Social Sciences and Humanities Research Council of Canada³ for research on “*Le prisme de la culture d’entreprise et la protection des inventions et données*” (“The Prism of Corporate Culture and the Protection of Inventions and Data”). My work on this thesis was supported by the grant, as I assisted Professor

² See Margaret Ann Wilkinson, “What is the Role of New Technology in Tensions in IP?,” (Presentation delivered at the International Association for the Advancement of Teaching and research in Intellectual Property [ATRIP], Montpellier, Monday July 7, 2014), online: <http://law.uwo.ca/about_us/our_people/PDFs/Wilkinson_ATRIP_Montpellier_2014.pdf>. See also: Margaret Ann Wilkinson, “What is the role of new technologies in tensions in Intellectual Property?,” in Tana Pistorius (ed) *Intellectual Property Perspectives on the Regulation of Technologies* [ATRIP Intellectual Property Law Series] (Cheltenham, UK: Edward Elgar) (in press). My thesis also builds upon my work on personal data protection in 2015, which culminated in my paper entitled “Balancing Individual and Collective Interests: Disclosure of Personal Health Information in Public Health Emergencies,” for which I was awarded the *J.S.D. Tory Writing Prize*.

³ Social Sciences and Humanities Research Council [SSHRC] Insight Grant 435-2016-1638, funded through the Faculty of Law at Western University under Professor Wilkinson’s supervision. I was the first “graduate research assistant” to be supported under this grant.

Wilkinson with research⁴ under this grant: this thesis forms part of the initial output from the four-year research program that is being supported by the grant.

The reality of an individual's right to control his or her personal data raises an important question in the context of clinical trials over the control and access to clinical data. Specifically, **does the data exclusivity right of pharmaceutical companies either operate consistently with or abrogate an individual's right to personal data protection in the clinical trial context?** To answer this question, this thesis will examine three constructs: 1) the legislative regulation of clinical trials; 2) the data exclusivity right of pharmaceutical companies; and 3) the individual's right to personal data protection. This thesis will accordingly explore the tension between the interests of pharmaceutical companies in maintaining confidentiality of data produced in clinical trials and the interests of the public in accessing this data to promote and protect public health.

Chapter One of this thesis offers an introductory discussion with respect to the legal regulation of pharmaceutical innovation, data exclusivity, and personal data protection. In particular, this chapter will briefly introduce and discuss the following matters: the history of Canadian regulatory requirements for the sale of new drugs; the movement of intellectual property rights into the international trade environment and the protection of confidential information therein; the notion of data exclusivity as a limitation on the permanent secrecy of confidential information; the need for personal

⁴ Together with JD student Colin Hyslop, I supported Professor Wilkinson in the preparation of her paper entitled "The Subject of Data and Intellectual Property in It: Do They Compete for Legal Priority?" (Presentation delivered at the 2017 Canadian IP Scholars' Workshop, Ottawa, 10 May 2017) [unpublished]. I was also a Discussant for the session in which the paper was presented. Professor Wilkinson's work on this paper (and her chapter forthcoming in the monograph that will flow from it) was directly supported by Social Sciences and Humanities Research Council Insight Grant 435-2016-1638 and the entire workshop, organized by Professors Goudreau and Wilkinson, was supported through a 2017-2018 SSHRC Connections Grant for "*Nouveaux paradigmes en propriété industrielle (New Paradigms in Industrial Property)*."

data protection laws to safeguard the confidentiality of personal information in the face of increased computerization; and how modern information technology facilitates techniques that enable previously “anonymized” data to be re-identified.

Chapter Two provides the theoretical and historical background to the main constructs that are addressed in this thesis and provides a review and discussion of the literature and Canadian case law surrounding confidential information, data exclusivity, and personal data protection. The nature of these constructs will be explored both as individual concepts and in terms of how they all relate to one another in the context of Canada’s legislative regime that regulates clinical trials and public health with respect to new drugs.

Chapter Three consists of a technical discussion of Canada’s legislative regimes for data exclusivity and personal data protection. First, this discussion will involve a review of data exclusivity laws in Canada and the flow of information under them. Second, an analysis of personal health information protection legislation will occur in order to explore whether there is a conflict between data exclusivity and personal data protection with respect to patient health information in clinical trial data. The definition of “personal health information” will be discussed in terms of its meaning under different personal health information statutes and its relationship to the notion of individual identifiability. Since current information technology has rendered complete anonymity to be impossible, this chapter emphasizes the importance of clarifying what it means for information to be identifiable. Through legislative analyses, this chapter will demonstrate that data exclusivity and personal data protection operate consistently with each other under Canadian law and that, despite any anonymization of patient data, personal data

protection applies to this data in clinical trials. Because of this latter finding, individual clinical trial participants retain their rights to control their personal health information. In this way, this chapter will also demonstrate that there is potential for conflict between the legislative regimes of data exclusivity and personal data protection.

Chapter Four answers the research question of this thesis and provides a list of findings in conclusion. These findings are subsequently discussed in the context of recommendations for future research.

Chapter 1 – Historical Background of Constructs

1.1. Historical Overview of Drug Regulation

In Canada, drug manufacturers must satisfy federal legislative requirements that “prescribe the standards of composition, strength, potency, purity, quality or other property” of drugs.⁵ For example, in order to sell or advertise a new drug in Canada, a drug manufacturer must receive a notice of compliance (NOC) after submission of evidence to the government which enables the government to assess the safety and efficacy of the drug.⁶ Clinical trials play a key role in the evidentiary record for efficacy and safety: these investigations are conducted to discover or verify clinical, pharmacological, or pharmacodynamics effects of drugs and identify possible adverse effects.⁷ Clinical trials generate unique information about a new drug, and data exclusivity protection, which constitutes a key focus of this thesis, refers to the temporary, exclusive rights to the information generated in clinical trials.⁸

The implementation of national regulatory requirements for drugs, such as those found in Canada’s *Food and Drug Regulations*,⁹ ultimately arose from the need to ensure the quality and safety of medicines, thereby reflecting a gradual evolution in the legislative protection of public health. Lembit Rägo and Budiono Santoso note that two major events catalyzed the development of the regulation of medicines.¹⁰ In 1937, over 100 people in the United States died following the use of a sulfanilamide elixir which

⁵ See *Food and Drug Regulations*, CRC, c 870, s A.01.002 [*Food and Drug Regulations*].

⁶ See *ibid.* The regulatory approval process for new drugs will be discussed in Chapter Three.

⁷ *Ibid.*, s C.05.001.

⁸ This thesis focuses solely on data exclusivity for pharmaceutical products. Data exclusivity will be subsequently explored in further detail in Chapters Two and Three.

⁹ *Food and Drug Regulations*, *supra* note 5.

¹⁰ Lembit Rägo & Budiono Santoso, “Drug Regulation: History, Present and Future,” in *Drug Benefits and Risks: International Textbook of Clinical Pharmacology*, revised 2nd ed, CJ van Boxtel, B Santoso & IR Edwards, eds, (IOS Press and Uppsala Monitoring Centre, 2008), 65-77 [Rägo & Santoso].

used diethylene glycol without any safety testing, thereby instigating the introduction of premarket notification requirements for new drugs.¹¹ The worldwide thalidomide disaster constituted the second catastrophe that influenced the development of a regulatory system for medicines: thalidomide, a sedative and hypnotic, was introduced in 46 different countries worldwide between 1958 and 1960 and resulted in approximately 10,000 babies being born with various deformities.¹² Following this tragedy, the Council of the European Economic Community approved Directive 65/65, which required that “no proprietary medicinal product may be placed on the market in a Member State unless an authorization has been issued by the competent authority of that Member State.”¹³ The need for further pharmaceutical regulatory harmonization to facilitate the availability of safe, effective, and quality drugs ultimately led to the establishment in 1990 of the International Council on Harmonization of Technical Requirements for the Registration of Pharmaceuticals for Human Use (ICH).¹⁴ This collaborative initiative, of which Canada is currently a “standing regulatory member,” focuses primarily on technical requirements for new, innovative medicines.¹⁵

The *Food and Drug Regulations* currently provide the only legally binding environment under which clinical trials are conducted in Canada. Guidance on the conduct of research, including clinical trials, can be found in the 2014 *Tri-Council Policy*

¹¹ *Ibid* at 65.

¹² *Ibid*.

¹³ EEC, *Council Directive 65/65/EEC of 26 January 1965 on the approximation of provisions laid down by law, regulation or administrative action relating to proprietary medicinal products*, [1965] OJ 022, P 0369 – 0373 at art 3, available online: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31965L0065:EN:HTML>> (accessed June 24, 2017).

¹⁴ Răgo & Santoso, *supra* note 10 at 66.

¹⁵ See ICH, *Current and Standing Members* (June 2017), online: <<http://www.ich.org/about/membership.html>> (accessed June 24, 2017).

Statement: Ethical Conduct for Research Involving Humans (“TCPS 2”).¹⁶ This policy is administered through the research ethics boards of institutions that receive funding from three federal agencies: the Canadian Institutes of Health Research (CIHR), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Social Sciences and Humanities Research Council (SSHRC). These agencies all require, as a condition of funding, that researchers and their institutions apply the ethical principles and articles contained in the TCPS 2.¹⁷

Individual consent to participation in research is a key principle of the TCPS 2 and applies generally to any research involving human participants. According to article 3.1 of the TCPS 2, research participants must give their consent voluntarily,¹⁸ and this consent can be withdrawn at any time.¹⁹ The data collected about a participant is also relevant to the principle of informed consent to participation in research. The TCPS 2 states that informed consent involves giving participants an indication about the information that will be collected about them, the purpose of collection, anticipated uses of the data, and information about who may have a duty to disclose information and to whom disclosure can be made.²⁰ For example, according to the TCPS 2, a participant

¹⁶ Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, December 2014, online: <http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf> [TCPS 2].

¹⁷ *Ibid* at 3. This policy applies only to investigators who are typically researchers and their institutions: investigators are distinct from clinical trial sponsors, as can be seen in Table 3 in Chapter Three.

¹⁸ *Ibid*, art 3.1(a):

Consent shall be given voluntarily.

¹⁹ *Ibid*, art 3.1(b):

Consent can be withdrawn at any time.

²⁰ *Ibid*, art 3.2:

...The information generally required for informed consent includes...(i) an indication of what information will be collected about participants and for what purposes; an indication of who will have access to information collected about the identity of participants, a description of how confidentiality will be protected (see Article 5.2), a description of the

who withdraws consent is also able to request the withdrawal of his or her data from the study.²¹ However, the TCPS 2 also acknowledges that there may be circumstances which do not allow withdrawal of participant data: the TCPS 2 specifically cites the anonymization of personal information and its subsequent addition to a data pool as an example of situations in which the withdrawal of data may not be possible.²² Nevertheless, since the TCPS 2 is not law,²³ legislated requirements will determine whether or not participant data remains in a clinical trial dataset.²⁴ This thesis thus focuses exclusively on the legislated aspects of clinical trials.

In light of the principle of informed consent to research, it might be tempting to conclude that, since the patient is aware of the consequences of participation in research, a patient loses any individual rights of control that may have been conferred by personal data protection legislation by virtue of signing a consent form for participation in the research. However, consent does not reach the binding level of contract, and even in the case of the stronger legal imperative of contract law, the recent Supreme Court of Canada decision, *Douez v. Facebook* (“*Douez*”),²⁵ establishes that organizations cannot oust

anticipated uses of data; and information indicating who may have a duty to disclose information collected, and to whom such disclosures could be made.

²¹ *Ibid*, art 3.1(c):

If a participant withdraws consent, the participant can also request the withdrawal of their data or human biological materials.

²² *Ibid*, art 3.1(c):

...In some research projects, the withdrawal of data or human biological materials may not be possible (e.g., when personal information has been anonymized and added to a data pool).

²³ *Ibid* at 16: The TCPS 2 states that researchers are responsible for “ascertaining and complying with all applicable legal and regulatory requirements with respect to consent and the protection of privacy of participants.” Where researchers experience a tension between the requirements of the law and the guidance of the ethical principles in the TCPS 2, “researchers should strive to comply with the law in the application of ethical principles.”

²⁴ The issue of withdrawal of data by clinical trial participants will be addressed in Chapter Three.

²⁵ 2017 SCC 33 [*Douez*]. The seven-person Court was split 4-3 in this decision. Justice Karakatsanis wrote for herself and Justices Wagner and Gascon; together with Justice Abella, who wrote for herself, these four judges constituted the majority and held that the forum selection clause contained in Facebook’s Terms of

privacy legislation through contract. In *Douez*, the appellant was a resident of British Columbia and claimed that Facebook, Inc. (“Facebook”) infringed her privacy rights and those of other British Columbians in a manner contrary to British Columbia’s *Privacy Act*.²⁶ Facebook sought to have the action stayed on the basis of the forum selection clause contained in its “Terms of Use” (a contract between Facebook and its users).

Karakatsanis J., writing one of the majority judgments in the Supreme Court, noted that forum selection clauses are regularly enforced since they create certainty and security in transactions,²⁷ and in commercial contexts, sophisticated parties that agree to forum selection clauses are deemed to have informed themselves about the risks of foreign legal systems and are deemed to have accepted those risks.²⁸ However, Karakatsanis J. also noted that “commercial and consumer relationships are very different,” since the “unequal bargaining power of the parties and the rights that a consumer relinquishes under the contract, without any opportunity to negotiate, may provide compelling reasons for a court to exercise its discretion to deny a stay of proceedings.”²⁹ Moreover, Karakatsanis J. characterized the issue in *Douez* in the

Use was unenforceable. Chief Justice McLachlin, with Justice Côté, wrote the dissent, for themselves and Justice Moldaver.

²⁶ RSBC 1996, c 373. The *Privacy Act* renders the violation of privacy an actionable tort. It is not a personal data protection statute, because it does not regulate the collection and handling of personal information by organizations. Unlike personal data protection statutes, the *Privacy Act* is not restricted to information about an identifiable individual: according to section 1(3), the “nature, incidence, and occasion of the act or conduct” and the relationship between the parties must be considered in order to determine “whether the act or conduct of a person is a violation of another’s privacy.” Furthermore, since section 1(4) states that eavesdropping or surveillance may constitute violations of privacy, the *Privacy Act* encompasses the individual’s right to refuse to disclose any information that he or she wishes to keep secret, which includes (but is not limited to) personal information.

²⁷ *Douez*, *supra* note 25, per Karakatsanis J. at para 24.

²⁸ *Ibid* at para 31.

²⁹ *Ibid* at para 33.

following language: “At issue in this case is Ms. Douez’s statutory privacy right. Privacy legislation has been accorded quasi-constitutional status.”³⁰

Through this reasoning and the concurring reasoning of Abella J., the majority of the Supreme Court judges hearing this case found that, although the *Privacy Act* does not specifically override the forum selection clause in a contract, the inequality of bargaining power between the parties gave Facebook the “unilateral ability to require that any legal grievances Ms. Douez had could not be vindicated in British Columbia,” which conferred an unfair procedural benefit upon Facebook.³¹ Abella J., concurring, noted a gross imbalance in bargaining power between Facebook, a multi-national corporation, and Douez, a private citizen, who “had no input into the terms of the contract and, in reality, no meaningful choice as to whether to accept them given Facebook’s undisputed indispensability to online conversations.”³² Abella J. found that the facts of the case satisfied the conditions for application of the doctrine of unconscionability.³³ Thus, the Supreme Court held that the forum selection clause in the contract between Facebook and Douez was unenforceable and therefore that the law of British Columbia, including its *Privacy Act*, would apply.

While *Douez* occurred in the context of a consumer contract, clinical trial participants most certainly face unequal bargaining power with respect to the entities that conduct clinical trials, particularly when these entities are pharmaceutical companies.

Aside from the obvious imbalance in financial resources, the patient’s decision to

³⁰ *Ibid* at para 59. While the British Columbia *Privacy Act* is not a personal data protection statute, Karakatsanis J. cited, in support of her point that “privacy legislation [is] quasi-constitutional,” *inter alia*, a Supreme Court decision based upon a personal data protection statute: *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 65-66.

³¹ *Douez*, *supra* note 25, per Abella J. at para 116.

³² *Ibid* at para 111.

³³ *Ibid* at para 115.

participate in a clinical trial may be heavily influenced by the need for treatment of a particular medical condition, such that it may not be a meaningful choice at all. Although the primary goal of clinical research is to produce generalizable scientific knowledge, some clinical investigators argue that the purpose of this research also includes ensuring state-of-the-art therapy for participants.³⁴ In this way, the administration of an experimental drug can be viewed “both as a means to learn about its safety and efficacy *and* as a therapeutic option.”³⁵ This perspective appears to be in accordance with that of organizations such as the Canadian Cancer Society, which lists the following potential benefits of participation in a clinical trial: the receipt of “state-of-the-art cancer care;” the possibility that the participant may be “the first to benefit from a new and effective treatment;” the possibility that the participant “may undergo an effective new treatment that has fewer side effects than standard treatment”; and, regardless of the outcome of the trial, “helping scientists answer important questions about cancer” which “may contribute new knowledge about cancer and eventually help others with the disease.”³⁶ Therefore, while certain information must be collected and retained from patients in order to meet the goals of the clinical trial, the “price” for this treatment would, especially in light of *Douez*, be unlikely to be considered to include relinquishing the individual’s statutory rights to control his or her personal information.

³⁴ Gail E Henderson et al, “Clinical Trials and Medical Care: Defining the Therapeutic Misconception” (2007) 4 PLoS Medicine 1735 at 1736. Henderson et al note that there is some conceptual disagreement as to the true purpose of a clinical trial: while some clinical researchers argue that the sole purposes of a clinical trial are to further the progress of science and help future patients, others argue that helping patients enrolled in a trial can serve as a legitimate additional purpose of a clinical trial.

³⁵ *Ibid* at 1737.

³⁶ Canadian Cancer Society, *Why Participate?* online: < <http://www.cancer.ca/en/about-us/our-research/clinical-trials-we-are-funding/?region=on> > (accessed August 6, 2017).

Since drug research and development has important consequences for the life sciences,³⁷ Elina Petrova has observed that the pharmaceutical industry faces enormous pressure to innovate, because “no other industry is expected to affect how long people can live or how fast they recover from an illness.”³⁸ On the other hand, “no other industry can burn through billions of dollars and man-hours only to end up empty-handed, with not much to show for its vast expenditure, dedication, and effort.”³⁹ Pharmaceutical innovation has thus influenced intellectual property law-making, particularly at the international level, owing to a confluence of factors such as the public’s need for essential medicines and the need to protect the large-scale investments of powerful pharmaceutical companies in drug development.

1.2. The Movement of Innovation (and Confidential Information) into International Trade

In 1967, developed countries established the World Intellectual Property Organization (WIPO) in order to promote the harmonization of intellectual property laws.⁴⁰ WIPO administers two principal international intellectual property covenants, the *Paris Convention for the Protection of Industrial Property* (“*Paris Convention*”)⁴¹ and the *Berne Convention for the Protection of Literary and Artistic Works* (“*Berne*

³⁷ See Elina Petrova, “Innovation in the Pharmaceutical Industry: The Process of Drug Discovery and Development,” in M Ding et al, eds, *Innovation and Marketing in the Pharmaceutical Industry: Emerging Practices, Research, and Policies* (New York: Springer, 2014), 19-81 at 25 [Petrova]: According to Petrova, the Second World War instigated a worldwide “extraordinary need” for antibiotics. In response to market demands, pharmaceutical firms invested in unprecedented research and development programs. Firms thus acquired technical and managerial experience and the organizational capability to produce massive volumes of drugs, thereby forever altering the process of drug discovery and development.

³⁸ *Ibid* at 23.

³⁹ *Ibid*.

⁴⁰ Brook K Baker & Katrina Geddes, “Corporate Power Unbound: Investor-State Arbitration of IP Monopolies on Medicines – *Eli Lilly v. Canada* and the Trans-Pacific Partnership Agreement” (2015) 23 J Intell Prop L 1 at 6 [Baker & Geddes].

⁴¹ (1883) 828 UNTS 305, *revised*, July 14, 1967 [*Paris Convention*].

Convention”),⁴² which were both signed at the end of the nineteenth century and were updated at various conferences.⁴³ Although the *Paris Convention* and the *Berne Convention* represented the first efforts to set global standards with respect to intellectual property rights protections,⁴⁴ these conventions suffer from two major flaws in that they both lack detailed rules on the enforcement of intellectual property rights before national judicial and administrative authorities as well as a binding and effective mechanism to settle disputes between states.⁴⁵ WIPO thus has limited success in its efforts to create normative intellectual property rights standards.⁴⁶

Beginning in the 1970s, developed countries such as the U.S. faced increasing pressure from domestic intellectual property industries to combat widespread infringement and raise standards of protection worldwide, thereby improving their ability to compete in foreign markets.⁴⁷ In 1986, the contracting parties of the *General Agreement on Tariffs and Trade, 1947*⁴⁸ launched the Uruguay Round of Multilateral Trade Negotiations (“Uruguay Round”), which concluded in 1994 with the creation of the World Trade Organization (WTO).⁴⁹ At the urging of corporate intellectual property owners, the U.S. pressed for the inclusion of intellectual property issues in the 1986

⁴² (1886) 828 UNTS 221, revised, July 14, 1967 [*Berne Convention*].

⁴³ Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis*, 4th ed (London: Sweet & Maxwell/Thomson Reuters, 2012) at 10 [Gervais].

⁴⁴ Baker & Geddes, *supra* note 40 at 6.

⁴⁵ Gervais, *supra* note 43 at 10.

⁴⁶ *Ibid.*

⁴⁷ Laurence R Helfer, “Regime Shifting: The TRIPS Agreement and New Dynamics of International Intellectual Property Lawmaking” (2004) 29 *Yale J Int’l L* 1 at 12 [Helfer].

⁴⁸ 30 October 1947, 58 UNTS 187 (entered into force 1 January 1948) [*GATT 1947*]. This treaty was established after the Second World War to promote free trade.

⁴⁹ Margaret Ann Wilkinson, “Confidential Information and Privacy-Related Law in Canada and in International Instruments” in Chios Carmody, ed, *Is Our House in Order? Canada’s Implementation of International Law* (Montreal & Kingston: McGill-Queen’s University Press, 2010), 275-311 at 281 [Wilkinson, “Confidential Information”].

negotiating mandate of the Uruguay Round.⁵⁰ Corporate intellectual property owners, including those in the pharmaceutical industry, heavily influenced the shift of innovation and intellectual property rights away from the public international law environment of WIPO and into international trade. The connection between intellectual property rights and trade is subsequently reflected in the 1994 *North American Free Trade Agreement* (“NAFTA”)⁵¹ and the *Agreement on Trade-Related Aspects of Intellectual Property* (“TRIPS”),⁵² which was introduced in 1995. TRIPS now includes no fewer than seven categories of intellectual property rights.⁵³

Linking intellectual property rights protection to trade issues effectively facilitated a restructuring of dispute settlement rules, creating a system in which decisions are binding on all states, and the use of retaliatory sanctions is authorized if states do not offer compensation or alter domestic laws found to be incompatible with the World Trade Organization Agreement.⁵⁴ Member states that fail to enforce intellectual property rights under both TRIPS and NAFTA are subject to potential economic sanctions under each agreement. TRIPS facilitates a dispute mechanism⁵⁵ through the *General Agreement on*

⁵⁰ Helfer, *supra* note 47 at 21.

⁵¹ 17 December 1992, Can TS 1994 No 2 (entered into force 1 January 1994) [*NAFTA*]. This agreement brought together the economies of Canada, the U.S., and Mexico with the objectives of eliminating barriers to free trade and facilitating the cross-border movement of goods and services between the member countries.

⁵² April 15 1994, *Marrakesh Agreement Establishing the World Trade Organization*, Annex 1C, (as amended on 23 January 2017), 1869 UNTS 299, 33 ILM 1197 [*TRIPS*]. This thesis will focus mainly on intellectual property rights issues that arise with respect to TRIPS rather than NAFTA, owing to the broader global scope of TRIPS.

⁵³ *Ibid*, art 1(2):

For the purposes of this Agreement, the term "intellectual property" refers to all categories of intellectual property that are the subject of Sections 1 through 7 of Part II.

Sections 1 through 7 of Part II of TRIPS encompass the following: copyright and related rights; trademarks; geographical indications; industrial designs; patents; layout-designs (topographies) of integrated circuits; and protection of undisclosed information.

⁵⁴ Helfer, *supra* note 47 at 22.

⁵⁵ See *TRIPS*, *supra* note 52, art 64(1):

Tariffs and Trade, 1994 (“GATT 1994”)⁵⁶ and the WTO Dispute Settlement Understanding (“DSU”).⁵⁷ Article XXIII of GATT 1994 provides for certain courses of action if any contracting party considers that “any benefit accruing to it directly or indirectly under this Agreement is being nullified or impaired” through, for example, the failure of another contracting party to carry out its obligations.⁵⁸ If the circumstances are “serious enough to justify such action,” contracting parties may authorize the suspension of “concessions or obligations under this Agreement.”⁵⁹ Article 22 of the DSU contains the rules governing the suspension of concessions or obligations, and, within it, Article 22(3) provides a number of principles and procedures that complaining parties must apply: although complaining parties should first seek to suspend concessions or other obligations with respect to the same sector in which the nullification or impairment occurred,⁶⁰ parties are authorized to seek to suspend concessions or other obligations in other sectors under the same agreement⁶¹ or under another covered agreement.⁶² In this way, since TRIPS authorizes sanctions involving sectors other than those for intellectual

The provisions of Articles XXII and XXIII of GATT 1994 as elaborated and applied by the Dispute Settlement Understanding shall apply to consultations and the settlement of disputes under this Agreement except as otherwise specifically provided herein.

⁵⁶ April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 UNTS 187, 33 ILM 1153 (1994) [*GATT 1994*].

⁵⁷ *Understanding on Rules and Procedures Governing the Settlement of Disputes*, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401, 33 I.L.M. 1226 (1994) [*DSU*].

⁵⁸ *GATT 1994*, *supra* note 56, art XXIII(1).

⁵⁹ *Ibid*, art XXIII(2).

⁶⁰ *DSU*, *supra* note 57, art 22(3)(a):

The general principle is that the complaining party should first seek to suspend concessions or other obligations with respect to the same sector(s) as that in which the panel or Appellate Body has found a violation or other nullification or impairment.

⁶¹ *Ibid*, art 22(3)(b):

If that party considers that it is not practicable or effective to suspend concessions or other obligations with respect to the same sector(s), it may seek to suspend concessions or other obligations in other sectors under the same agreement.”

⁶² *Ibid*, art 22(3)(c):

If that party considers that it is not practicable or effective to suspend concessions or other obligations with respect to other sectors under the same agreement, and that the circumstances are serious enough, it may seek to suspend concessions or other obligations under another covered agreement.

property, failing to carry out intellectual property obligations under TRIPS can result in far-reaching economic consequences. NAFTA provides for economic sanctions in a similar manner: Article 2019 of NAFTA directly authorizes the “suspension of benefits” for “measures” that do not conform to NAFTA.⁶³ In a manner similar to TRIPS, complainant parties under NAFTA are also authorized to apply sanctions in different economic sectors.⁶⁴

In addition to establishing binding dispute settlement mechanisms for intellectual property rights, the movement of innovation into international trade also created a new discourse with respect to the protection of confidential information. For instance, Margaret Ann Wilkinson notes that TRIPS used the texts of public international law treaties such as the *Paris Convention* and the *Berne Convention* as the threshold for patent protection and copyright protection, respectively, in the new international trade environment.⁶⁵ However, international parameters with respect to the protection of confidential information were introduced for the first time in the context of the “coercive” conditions of trade negotiations.⁶⁶ Confidential information is now protected

⁶³ NAFTA, *supra* note 51, art 2019(1):

If in its final report a panel has determined that a measure is inconsistent with the obligations of this Agreement or causes nullification or impairment in the sense of Annex 2004 and the Party complained against has not reached agreement with any complaining Party on a mutually satisfactory resolution pursuant to Article 2018(1) within 30 days of receiving the final report, such complaining Party may suspend the application to the Party complained against of benefits of equivalent effect until such time as they have reached agreement on a resolution of the dispute.

⁶⁴ *Ibid.*, art 2019(2):

In considering what benefits to suspend pursuant to paragraph 1: (a) a complaining Party should first seek to suspend benefits in the same sector or sectors as that affected by the measure or other matter that the panel has found to be inconsistent with the obligations of this Agreement or to have caused nullification or impairment in the sense of Annex 2004; and (b) a complaining Party that considers it is not practicable or effective to suspend benefits in the same sector or sectors may suspend benefits in other sectors.

⁶⁵ Wilkinson, “Confidential Information,” *supra* note 49 at 282.

⁶⁶ *Ibid.*

as intellectual property under TRIPS and NAFTA,⁶⁷ thereby reflecting the importance of confidential information with respect to innovation and, consequently, to national economic interests.

1.3. Data Exclusivity: Relationship to Intellectual Property and Confidential Information

Although the protection of confidential information may be advantageous to the person or business entity that is holding the information,⁶⁸ the philosophical underpinnings of the protection remain unclear. Indeed, as an aspect of law, the normative basis for protecting confidential information has differed.⁶⁹ At common law, confidential information can be protected through contract, and in equity, confidentiality can be buttressed by the concept of fiduciary obligations.⁷⁰ In Canada, the first clear recognition of the protection of confidential information occurred in 1989 with respect to breach of the duty of confidence, but the Supreme Court of Canada has declined to precisely classify the basis of protection.⁷¹

The protection of confidential information is directly relevant to data exclusivity for pharmaceutical products. Obligations of data exclusivity originate from TRIPS and NAFTA, under which member states are required to protect “undisclosed” pharmaceutical test data against disclosure.⁷² Data exclusivity is thus directly related to

⁶⁷ The protection of confidential information as intellectual property will be explored later in Chapter Two.

⁶⁸ Gregory Hagen et al, *Canadian Intellectual Property Law: Cases and Materials*, (Toronto: Emond Montgomery Publications, 2013) at 573 [Hagen et al]: For example, a secret recipe, client list, or technological drawings may be “all the more valuable” if kept secret by the holder, particularly with respect to competitors of the holder.

⁶⁹ *Ibid* at 576.

⁷⁰ *Ibid* at 575-576.

⁷¹ See *International Corona Resources Ltd v LAC Minerals Ltd*, [1989] 2 SCR 574 [*LAC Minerals*].

⁷² See *TRIPS*, *supra* note 52, art 39(3) and *NAFTA*, *supra* note 51, art 1711(5)-(6).

states' regulatory regimes for new drugs, and Canada introduced its first data exclusivity framework in 1995.⁷³

Although pharmaceutical companies typically seek patent protection to protect a new, innovative drug, the issuance of the patent for the drug does not discharge a pharmaceutical company's legal obligation to obtain market approval where required from a state government. Because of the requirement for market approval, and although a patent grants an innovator the right to distribute an invention,⁷⁴ a pharmaceutical company cannot use this patent-related right of distribution unless it first undertakes the extra step of receiving regulatory approval from the state government.⁷⁵ Data exclusivity can be defined as the temporary protection of clinical test data that is required to be submitted to a regulatory agency in order to prove the safety and efficacy of a new drug.⁷⁶ During the period of data exclusivity, only the innovator is permitted to rely on this data in an application for regulatory approval.⁷⁷ While a patent is typically filed before the start of clinical trials that generate safety and efficacy information,⁷⁸ the period of data exclusivity typically extends beyond the life of the patent and allows companies to recoup the cost of investment in generating the information for regulatory approval. In

⁷³ The law of data exclusivity in Canada will be explored in detail in Chapter Three.

⁷⁴ *Patent Act*, RSC 1985, c P-4, s 42 [*Patent Act*]:

Every patent granted under this Act shall...grant to the patentee and the patentee's legal representatives for the term of the patent, from the granting of the patent, the exclusive right, privilege and liberty of making, constructing and using the invention and **selling it to others** to be used, subject to adjudication in respect thereof before any court of competent jurisdiction [emphasis added].

⁷⁵ Arguably, the inability to distribute significantly weakens the utility of a patent in the pharmaceutical context, since distribution is the ultimate goal of any patent – a way to capitalize on the effort expended in innovation.

⁷⁶ Olasupo A Owoeye, "Data Exclusivity and Public Health under the TRIPS Agreement" (2015) 23 J L Info & Sci 106 at 108.

⁷⁷ See *Food and Drug Regulations*, *supra* note 5, s C.08.004.1(3).

⁷⁸ Dana P Goldman et al., "The Benefits From Giving Makers of Small Molecule Drugs Longer Exclusivity over Clinical Trial Data" (2011) 30 Health Affairs 84 at 85.

this way, data exclusivity operates independently from patent,⁷⁹ and one commentator has noted that both patent protection and data exclusivity create a temporary, monopoly situation that enables the recovery of costs incurred during drug discovery and development.⁸⁰

The data exclusivity framework that originates from TRIPS and NAFTA essentially placed the data generated in clinical trials into the realm of intellectual property. Intellectual property rights have been expressed as having a pre-defined scope, and within this scope, they negatively exclude the world and positively grant limited, exclusive rights to use the subject matter.⁸¹ Since intellectual property rights are intended to both stimulate and reward individual creativity, innovation, and investment,⁸² the reach of exclusivity and the requirements of intellectual property protection reflect a balance with respect to the public interest.⁸³ In light of this balance, temporary exclusive rights are viewed as the norm for classic intellectual property devices such as patent, copyright, and trademark.⁸⁴

However, whereas traditional intellectual property frameworks specifically encourage the dissemination of information in society, the protection of confidential information “does the opposite,”⁸⁵ because confidential information has the potential to remain secret forever.⁸⁶ Since confidential information does not have a public access

⁷⁹ See *Petrova*, *supra* note 37 at 31: For example, patent and data exclusivity may or may not run concurrently and they may not necessarily encompass the same claims.

⁸⁰ *Ibid* at 32.

⁸¹ Alexander Peukert, “Individual, multiple and collective ownership of intellectual property rights – which impact on exclusivity?” in *The Structure of Intellectual Property Law: Can One Size Fit All?*, Annette Kur & Vytautas Mizaras, eds, (Cheltenham, UK & Northampton, USA: Edward Elgar Publishing, 2011).

⁸² *Ibid* at 197-198.

⁸³ *Ibid* at 199-200.

⁸⁴ *Ibid* at 200.

⁸⁵ Hagen et al, *supra* note 68 at 573.

⁸⁶ A more detailed discussion of confidential information will occur in Chapter Two.

aspect at all, it does not appear to lie within the classic definition of intellectual property that includes a “bargain” between an intellectual property rights holder and the public interest.⁸⁷ As this thesis will demonstrate, however, data exclusivity places a limitation on the secrecy of clinical trial data. In doing so, data exclusivity functions in a manner similar to classic intellectual property devices. It grants a limited-term monopoly over the data from clinical trials: the flow of information is interrupted during the period of protection. With respect to the testing of new pharmaceutical products, data exclusivity ensures that innovators who invest money and effort into conducting clinical trials will have an initial opportunity to maintain the secrecy of valuable data, and competitors of these innovators will not be able to use the information for a given number of years in an application for regulatory drug approval, giving the innovators a competitive market advantage. The information subsequently becomes accessible to other drug manufacturers following the expiration of the data exclusivity period, thereby ending the innovator’s ability to control the free flow of information. Data exclusivity thus requires an end to the confidentiality of information that would otherwise remain secret forever.⁸⁸

1.4. Personal Data Protection: Historical Overview

Beginning in the late 1970s with the emergence of global telecommunications and computerization, countries began to seek domestic legislative implementation of privacy values in light of the increased memory capacity, processing speed, and ubiquity of computers.⁸⁹ Since the portability of data between states was essential for ensuring that all nations could participate in the anticipated “information economy,” the Organization

⁸⁷ The “bargain” in intellectual property law will be explained and discussed in Chapter Two.

⁸⁸ The nuances of data exclusivity will be analyzed in Chapter Two.

⁸⁹ Margaret Ann Wilkinson, “Confidential Information,” *supra* note 49 at 283.

for Economic Cooperation and Development (OECD) first published the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*⁹⁰ (“OECD Privacy Guidelines”) in 1981 in order to both protect personal information and promote the free flow of data between countries.⁹¹ Member countries of the OECD, including Canada, are required to implement the OECD Privacy Guidelines, including the Basic Principles of National Application⁹² and are advised to adopt laws protecting privacy and to coordinate various government bodies through the development of national privacy strategies.⁹³ Importantly, according to the Individual Participation Principle under the OECD Privacy Guidelines, individuals have express rights to access their personal information and to “have the data erased, rectified, completed, or amended” in the event of a successful challenge to the collection of this data.⁹⁴

Canada accordingly enacted the *Privacy Act*,⁹⁵ which aims to provide individuals with a right of access to their personal information held by a federal government institution and to protect the privacy of individuals with respect to that information.⁹⁶ At the same time, however, Canada acknowledged the need for democratic openness with respect to the public accessibility of government documents and enacted the *Access to Information Act*⁹⁷ (“*Access Act*”). The *Privacy Act* and the *Access Act* together create a

⁹⁰ The 2013 OECD Privacy Guidelines now constitute the first update to the Guidelines since 1980 but leave intact the original “Basic Principles”: see OECD, *2013 OECD Privacy Guidelines*, <<https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>> (accessed June 24, 2017).

⁹¹ Wilkinson, “Confidential Information,” *supra* note 49 at 283.

⁹² The eight Basic Principles are as follows: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability. See Part Two of the Organization for Economic Cooperation and Development, *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (2013), available online: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [*OECD Guidelines*].

⁹³ *Ibid*, Part Five.

⁹⁴ *Ibid*, Part Two at para 13.

⁹⁵ RSC, 1985, c P-21 [*Privacy Act*].

⁹⁶ *Ibid*, s 2.

⁹⁷ RSC 1985, c A-1 [*Access Act*].

balance between access to information generally and the confidentiality of certain information held by federal institutions in the public sector.

The provinces followed suit generally by creating “omnibus” statutes that combined access and personal data protection regimes in single statutes.⁹⁸ Both provincial and federal legislators also perceived a need to address questions of an individual’s control over his or her personal information held by private sector organizations and a need to ensure that this information was adequately protected.⁹⁹ Quebec was the first Canadian jurisdiction to adopt personal data protection legislation for the private sector,¹⁰⁰ which has been in force since 1994. More recently, the *Personal Information Protection and Electronic Documents Act*¹⁰¹ (“PIPEDA”) was passed by the federal government in 2000 and protects personal information with respect to federally regulated private sector organizations and organizations that engage in “commercial activities.”¹⁰² The need for comprehensive regulation of the collection, use, and disclosure of personal information in the hands of both public and private sector organizations has ultimately led to a proliferation of personal data protection statutes across Canada. All Canadian jurisdictions have now legislated in the area of public sector personal data protection.¹⁰³ In addition to Quebec and the federal government, Alberta¹⁰⁴ and British Columbia¹⁰⁵ have their own private sector personal data protection laws.

⁹⁸ See for example, Ontario’s *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 [FIPPA].

⁹⁹ Mark Perry & Margaret Ann Wilkinson, “The Creation of University Intellectual Property: Confidential Information, Data Protection, and Research Ethics” (2010) 26 CIPR 93 at 96 [Perry & Wilkinson].

¹⁰⁰ *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 [QC Act].

¹⁰¹ SC 2000, c 5 [PIPEDA].

¹⁰² *Ibid*, s 2(1).

¹⁰³ See Perry & Wilkinson, *supra* note 99.

¹⁰⁴ *Personal Information Protection Act*, SA 2003, c P-6.5 [AB PIPA].

¹⁰⁵ *Personal Information Protection Act*, SBC 2003, c 63 [BC PIPA].

Personal data protection specifically designed for the health context has also now been enacted by nearly all Canadian jurisdictions.¹⁰⁶

1.5. Personal Data Protection: Questions of Identifiability and Relationship to Data Exclusivity

The immense computing and processing power of modern information technology in 2017 raises personal data protection issues that did not exist when Canada's data exclusivity framework was first introduced in 1995. For instance, privacy issues in clinical research were, in 1995, typically addressed through the protection of the identities of the research participants because patient data underwent anonymization (or de-identification) using techniques to aggregate the data into large sets which meant the removal of identifiers, such as individual names, not necessary for statistical analyses.¹⁰⁷ However, advances in information technology and storage have now resulted in the ability to perform large-scale analyses of vast data sets, which in turn decreases the need to "strip" data of identifiers in the first place and, if stripped, increases the likelihood for re-identification of data that has been rendered anonymous: identifying information can now be produced from non-identifying information because of the potential to link multiple data sets together.¹⁰⁸

The risk of re-identification through modern information technology such as data linkage calls into question the meaning of individual identifiability with respect to the

¹⁰⁶ Personal health information protection laws constitute the focus of this thesis with respect to personal data protection and will be discussed in detail in Chapter Three.

¹⁰⁷ Khaled El Emam & Bradley Malin, *Concepts and Methods for De-Identifying Clinical Trial Data* (2014), Paper commissioned by the Committee on Strategies for Responsible Sharing of Clinical Trial Data, at 2, available online: <<http://nationalacademies.org/hmd/~/media/Files/Report%20Files/2015/SharingData/ElEmamandMalin%20Paper.pdf>> (accessed June 2017).

¹⁰⁸ Data matching will be fully addressed in Chapter Three, along with the personal health information protection statutes that address this technique.

application of personal data protection laws in the context of clinical trials. As will be discussed in section 3.3 in Chapter Three of this thesis, large amounts of personal health information, including an individual's weight, blood pressure, and medical history, are collected from individual participants in the course of a clinical trial, and clinical trial practices mandate the retention of records that would identify each individual participant in the case of adverse events.¹⁰⁹ The ability to identify clinical trial participants in this manner raises the question of whether personal data protection actually still applies to "de-identified" clinical trial data, since this data is simply assumed to be truly anonymous but may in fact not be so in light of current technological realities.

However, if individuals retain rights of control to their data in clinical trials in accordance with personal data protection principles, each individual's rights of control could conflict with the rights of drug manufacturers with respect to data exclusivity. Furthermore, if the result of this conflict is such that personal data protection *prevails* over data exclusivity, this situation would challenge Canada's international obligations under TRIPS and NAFTA and would place Canada in a difficult position in terms of its simultaneous attempts at enforcing rights under the legislative regimes of both personal data protection and data exclusivity. Owing to the potential struggle for control over information in clinical trials, this thesis seeks to determine whether data exclusivity operates consistently with personal data protection in Canadian law.

1.6. Conclusion

The research question of this thesis arises in the context of Canada's obligations to implement two potentially conflicting legislative regimes in the context of the public

¹⁰⁹ See *Food and Drug Regulations*, *supra* note 5, s C.05.012.

health regulation of drugs. On one hand, data exclusivity originates from the international trade environment in a “top-down” manner, under which member states are required to enforce intellectual property rights through their domestic laws. A member state’s failure to adequately implement these rights can result in negative economic consequences at the national level. On the other hand, while personal data protection originates from an international instrument and gives an individual the right to control his or her personal data, personal data protection has arisen across Canada in a largely “bottom-up” manner with the implementation of legislative personal data protection regimes occurring at both the provincial and national levels.

The protection of confidential information serves as common ground with respect to both data exclusivity and personal data protection. Confidentiality of information creates a potentially permanent barrier to the free flow of information, and an important goal of both data exclusivity and personal data protection concerns the secrecy of information. Nevertheless, both these regimes of data exclusivity and personal data protection transcend confidential information protection since they each only maintain secrecy of information to a certain extent. Data exclusivity functions in a manner akin to intellectual property protection and provides a limited-term monopoly on secrecy. Legislated personal data protection controls are imposed on organizations for the benefit of individuals, which, unlike the law of confidential information, apply whether or not the information was confidential in the first place and regardless of an individual’s awareness of the collection of the information.¹¹⁰

Modern information technology has also called into question the understanding of identifiability. Anonymization is closely related to the question of whether the

¹¹⁰ Perry & Wilkinson, *supra* note 99 at 96.

confidentiality of personal information can be ensured: if de-identified information can be re-identified and so constitutes identifiable information in a *factual* sense, such a finding has implications for an individual's right to control his or her personal information under personal data protection laws. This thesis thus examines whether data exclusivity operates consistently with personal data protection or instead abrogates an individual's right to personal data protection in the clinical trial context.

Chapter Two – Theoretical Background of Constructs

2.1. Introduction

This chapter discusses the theoretical backgrounds of confidential information, data exclusivity, and personal data protection. Examination of the first construct, confidential information, will involve an exploration of the nature of confidential information by reviewing case law and academic scholarship, particularly with respect to the duty of confidence. The regulation of the sale of drugs will also be explored to illustrate that clinical trials are heavily regulated in order to protect public health. Within this context, a recent Supreme Court of Canada decision, *Merck Frosst Canada Ltd. v. Canada (Minister of Health)*,¹¹¹ will be used to demonstrate the tension between the access and secrecy of confidential information in the pharmaceutical context. To explore the second construct, data exclusivity protection, the discussion will consist of a brief description of the origins of data exclusivity in international trade agreements to provide a contextual framework. In this context, the nature and purpose of data exclusivity will be examined from the perspectives of supporters and opponents of data exclusivity. Finally, examination of the third construct, personal data protection, will involve a discussion of how personal data protection is related to, but distinct, from privacy law with respect to regulating the flow of information between individuals and organizations. The chapter ultimately concludes that, although personal data protection is relevant to data exclusivity, personal data protection has largely been excluded from the data exclusivity discourse.

¹¹¹ 2012 SCC 3, [2012] 1 SCR 23 [*Merck Frosst SCC*].

2.1.1. The Nature of Confidential Information: Excluding Others - The Importance of Confidential Information to Private Businesses

Exclusive rights to information ultimately result in a monopoly over use of the knowledge. In order to justify this exclusion, knowledge must be novel, unique, identifiable, or secret: mere ideas will not suffice to receive legal protection.¹¹² In particular, a company's ability to maintain secrecy over information pertaining to its technology may successfully delay a competitor from copying the technology, thereby giving the company a competitive market advantage.¹¹³ Intellectual property rights, which provide exclusive rights to activities including the manufacture, use, and sale of particular goods, are thus crucial business assets.¹¹⁴ For modern business organizations, the slightest advances in technology can give companies an enormous competitive advantage over their market rivals, and maintaining exclusive possession of valuable technical and commercial information can sometimes mean the difference between cornering a particular market and fighting for financial survival.¹¹⁵

Despite the present characterization of confidential information as intellectual property in the international trade environment,¹¹⁶ the type of intellectual property protection available for a particular thing is arguably determined by "the nature of the thing."¹¹⁷ Wilkinson has noted that the inclusion of confidential information under TRIPS and NAFTA marked the first time that confidential information has been classified as

¹¹² Gordon J Zimmerman, "Protecting the Value of Intellectual Property: The Basics" (2001) 2001 J Bus Valuation 201 at 201 [Zimmerman].

¹¹³ *Ibid* at 202.

¹¹⁴ *Ibid* at 201.

¹¹⁵ Robert Unikel, "Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets" (1998) 29 Loyola U Chicago L J 841 at 841.

¹¹⁶ See *TRIPS*, *supra* note 52, art 39 and *NAFTA*, *supra* note 51, art 1711.

¹¹⁷ Zimmerman, *supra* note 112.

intellectual property.¹¹⁸ There has been much uncertainty in legal scholarship with respect to the nature of confidential information and its proper characterization. Indeed, the philosophical base for its protection has remained unclear owing to the absence of legislative enactment and the lack of consistent judicial guidance.

2.1.2. The Nature of Confidential Information: A Question of Duty

According to Arnold Weinrib, writing in 1988,¹¹⁹ there is a *prima facie* case for recognizing confidential information as property.¹²⁰ However, at the very least, a dispute about the protection of confidential information will be based on the express or implied contractual obligation to maintain confidentiality of the information.¹²¹ In the absence of a contract, the relationship between the parties may give rise to a fiduciary obligation,¹²² in which misuse of information would constitute a breach of this obligation.¹²³

The existence of certain duties between parties has thus featured prominently in the discourse regarding the protection of confidential information. Duties may arise because of the exchange of valuable information between parties in a context in which the need for confidentiality has been made clear to the confidante.¹²⁴ The exchange of

¹¹⁸ Wilkinson, “Confidential Information,” *supra* note 49 at 282.

¹¹⁹ Arnold S Weinrib, “Information and Property” (1988) 38 UTLJ 117 [Weinrib].

¹²⁰ *Ibid.* Weinrib’s article was published one year before the Supreme Court of Canada released its decision in *International Corona Resources Ltd v LAC Minerals Ltd*, [1989] 2 SCR 574, which is a leading case on the protection of confidential information in Canada. This decision will be discussed in section 2.1.4 of this thesis.

¹²¹ *Ibid* at 128.

¹²² See *Can Aero v O’Malley*, [1974] SCR 592, 1973 CanLII 23. The defendants had wrongfully taken the benefit of a corporate opportunity in breach of a fiduciary duty. As Canaero’s “top management and not mere employees,” the defendants had a duty to their employer that, “unless enlarged by contract, consisted only of respect for trade secrets and for confidentiality of customer lists.” The Supreme Court of Canada thus held that the defendants had a fiduciary obligation to Canaero, “which in its generality betokens loyalty, good faith, and avoidance of a conflict of duty and self-interest.”

¹²³ Weinrib, *supra* note 119 at 128.

¹²⁴ Hagen et al, *supra* note 68 at 580.

valuable information causes the confiding party to be vulnerable if the information is divulged by the confidante, such that this exposure to risk leads to duties being imposed on the confidante.¹²⁵ It follows that the legal duty imposed based on the exchange of information is restricted both in terms of scope and duration, in which the duty endures only as long as the secret remains a secret and also pertains only to maintaining the secret and not to a wider, fiduciary relationship.¹²⁶

In this way, English and Canadian courts have observed a duty of confidence with respect to the protection of confidential information. The relevant English and Canadian case law will be explored in the sections below, in which this thesis will show that the law still remains uncertain as to the proper characterization of confidential information.

2.1.3. The Nature of Confidential Information: The Duty of Confidence in English Case Law

A leading authority for breach of confidence is the English case, *Saltman Engineering Co. v. Campbell Engineering Co.*,¹²⁷ in which Lord Greene uttered a classic articulation of the key characteristics of confidential information:

....The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch, or something of that kind, which is the result of work done by the maker upon materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process.¹²⁸

According to Lord Greene's statement, confidential information is knowledge that

¹²⁵ *Ibid.*

¹²⁶ *Ibid.*

¹²⁷ (1948) 65 RPC 203 (Eng CA); leave to appeal to House of Lords refused [*Saltman Engineering*].

¹²⁸ *Ibid* at 215.

is not public and can also constitute information which has resulted from an individual's unique mental labour. Confidentiality of information also persists independently from contract. If a contract is silent on the matter of confidence, there is an implied obligation to treat the confidential matter "in a confidential way," such that the obligation to respect confidence is not limited to cases where the parties are in a contractual relationship.¹²⁹ If a defendant uses confidential information, either directly or indirectly obtained from a plaintiff without the plaintiff's express or implied consent, the defendant will be guilty of an infringement of the plaintiff's rights.¹³⁰

Based on this reasoning, Lord Greene observed that, "contract or no contract," the defendants came into possession of the plaintiffs' drawings in light of the knowledge that this material belonged to the plaintiffs and was "obviously confidential matter."¹³¹ Moreover, by using the confidential drawings, the defendants managed to "dispense in certain material respects with the necessity of going through the process which had been gone through in compiling these drawings," thereby saving the defendants "a great deal of labour and calculation and careful draughtsmanship."¹³² The circumvention of the labour and production process that arose from the use of the confidential information thus constituted a breach of the duty of confidence, which was owed by the defendants to the plaintiffs, who were the "owners of the confidential matter."¹³³

Lord Greene in *Saltman Engineering* identified some important characteristics of confidential information. However, he did not expressly classify confidential information as property. Despite Lord Greene's use of proprietary language in referring to the

¹²⁹ *Ibid* at 211.

¹³⁰ *Ibid* at 213.

¹³¹ *Ibid* at 216.

¹³² *Ibid* at 215.

¹³³ *Ibid*.

plaintiffs as “owners” of the confidential material, this term may simply have referred to the *physical* documents that happened to contain the confidential information at issue.¹³⁴ Since *Saltman Engineering* concerned the duty of confidence and the relationship between the parties to the dispute, it is unclear as to whether a duty of confidence arises from an interest in the information itself or from other factors such as the relationship between the parties or the circumstances of the case.

The classic articulation of the duty of confidence can be found in the English case, *Coco v. AN Clark (Engineers) Ltd.*¹³⁵ Megarry J. agreed with Lord Greene’s comments in *Saltman Engineering*, in that the duty of confidence may exist where there is no contractual relationship between the parties. Accordingly, he observed that, where there is no contract, “the question must be one of what it is that suffices to bring the obligation into being.”¹³⁶ Megarry J. subsequently identified three essential elements of a breach of the duty of confidence: 1) the information must be of a confidential nature; 2) the information must have been communicated in circumstances importing an obligation of confidence; and 3) there must be unauthorized use of the information to the detriment of the party that communicated it.¹³⁷ With respect to the concept of confidentiality, Megarry J. echoed the views of Lord Greene in *Saltman Engineering*, in that a person’s ingenuity and innovative skill may impart a quality of confidentiality to an invention constructed from publicly available materials.¹³⁸ Megarry J. further concluded that “there must be some product of the human brain which suffices to confer a confidential nature

¹³⁴ *Ibid* at 213:

Without going further into the matter, it seems to me that the existence of a confidential obligation in relation to those drawings, as between *Saltman* and the Defendants, is abundantly proved.

¹³⁵ [1968] FSR 415 (HCJ) [*Coco*].

¹³⁶ *Ibid* at 419.

¹³⁷ *Ibid* at 419.

¹³⁸ *Ibid* at 420.

upon the information.”¹³⁹ It is through the exertion of mental effort and the creative thought process by which “something new and confidential may have been brought into being.”¹⁴⁰

In this way, one commentator has noted that the action for breach of confidence essentially protects original thought processes and creative efforts.¹⁴¹ In accordance with the reasoning in *Coco*, as well as *Saltman Engineering*, breach of confidence will occur when the defendant takes unfair advantage of information that has been disclosed to him or her, thereby saving the “time, trouble, and expense of going through the same process.”¹⁴² However, although the three-step test enunciated by Megarry J. in *Coco* is certainly informative with respect to the factors that amount to breach of confidence, Megarry J. was concerned mostly with concept of *confidentiality* alone, rather than the *nature of confidential information*. Accordingly, he did not attempt to classify confidential information into a specific category and so did not provide further guidance as to the proper characterization of confidential information.

2.1.4. The Nature of Confidential Information: The Protection of Confidential Information in Canadian Case Law

In Canada, the nature of confidential information has been raised in case law in both the criminal and civil contexts. For example, the Supreme Court of Canada in *R. v. Stewart*¹⁴³ examined the question of whether confidential information can be the subject

¹³⁹ *Ibid.*

¹⁴⁰ *Ibid.*

¹⁴¹ Alexander J Penk, “Confidential Information in a Commercial Context: An Analysis of “Use” of Confidential Information and the Availability of a Proprietary Remedy for Breach of Confidence” (2000) 9 Auckland U L Rev 470 at 475.

¹⁴² *Ibid.*

¹⁴³ [1988] 1 SCR 963 [*Stewart* SCC].

of theft under the *Criminal Code* and ultimately held that confidential information does not qualify as property for the purposes of the law of theft. However, Lamer J., writing for the Court, also commented on the nature of confidential information in the context of civil law with respect to this information's potential characterization as property:

It can be argued...that confidential information is property for the purposes of civil law. Indeed, it possesses many of the characteristics of other forms of property: for example, a trade secret, which is a particular kind of confidential information, can be sold, licensed or bequeathed, it can be the subject of a trust or passed to a trustee in bankruptcy. In the commercial field, there are reasons to grant some form of protection to the possessor of confidential information: it is the product of labour, skill and expenditure, and its unauthorized use would undermine productive efforts which ought to be encouraged. As the term "property" is simply a reference to the cluster of rights assigned to the owner, this protection could be given in the form of proprietary rights.¹⁴⁴

The above statement echoes the perspective of Weinrib, mentioned previously, who asserted that confidential information is property. However, this statement nevertheless fell far short of clarifying the nature of confidential information in any definitive manner. Lamer J. merely declared that "it can be argued" that confidential information *can* be classified as property, which certainly does not translate into an assertion that "confidential information *should* be classified as property." Rather than settling the law, Lamer J. simply described the inconsistencies in judicial decision-making with respect to the treatment of confidential information as property. In the civil context, Lamer J. noted that Canadian law¹⁴⁵ does protect confidential information, but the legal basis for doing so has not been clearly established by the courts: while some cases treat confidential information as property that entitles an owner to exclude others

¹⁴⁴ *Ibid* at para 23.

¹⁴⁵ For example, see *International Corona Resources Ltd v LAC Minerals Ltd*, (1987) 62 OR (2d) 1, aff'd (1986) 53 OR 2(d) 737.

from use,¹⁴⁶ the courts have also recognized certain rights to confidential information that arise from the equitable obligation of good faith.¹⁴⁷ Furthermore, Lamer J. noted that the protection afforded to confidential information in most civil cases arises “more from an obligation of good faith or a fiduciary relationship than from a proprietary interest,”¹⁴⁸ concluding that “no Canadian court has so far conclusively decided that confidential information is property, with all the civil consequences that such a finding would entail.”¹⁴⁹ Lamer J. thus raised, but ultimately did not answer, the question as to whether confidential information constitutes property.

Wilkinson has noted that the Supreme Court of Canada has ultimately declined to specifically characterize confidential information.¹⁵⁰ *International Corona Resources Ltd v. LAC Minerals Ltd.*¹⁵¹ is a leading case¹⁵² on breach of confidence and fiduciary duty in the commercial context and the appropriate remedies that arise from such breaches. The appellant, LAC Minerals Ltd. (“LAC”), had expressed interest in joining the respondent, International Corona Resources Ltd. (“Corona”), in exploring a property that Corona suspected had gold. Information that was not available to the public was revealed to LAC during meetings to discuss the venture. Subsequently, LAC used this information to make an offer for the property and then acquired and mined it. Although the ultimate finding of

¹⁴⁶ *Stewart SCC*, *supra* note 143 at para 23, referring to *Aas v Benham*, [1891] 2 Ch 244 (Eng CA); *Exchange Telegraph Co v Gregory & Co.*, [1896] 1 QB 147.

¹⁴⁷ *Ibid* at para 23, referring to *Saltman Engineering*, *supra* note 127; *Seager v Copydex*, [1967] 2 All ER 415 (Eng CA); *Phipps v Boardman*, [1967] 2 AC 46 (UK HL).

¹⁴⁸ *Ibid* at para 24.

¹⁴⁹ *Ibid*.

¹⁵⁰ Wilkinson, “Confidential Information,” *supra* note 49 at 282.

¹⁵¹ *LAC Minerals*, *supra* note 71.

¹⁵² *Ibid*. This case was heard by only five of the nine judges of the Supreme Court of Canada, and the only issue on which all the judges agreed was that the appellant, LAC, was liable for breach of confidence, and that the traditional test in *Coco* applied.

a fiduciary relationship between the parties divided the court,¹⁵³ all five judges agreed that a breach of confidence had occurred. However, despite the fact that Lamer J. was also one of the deciding judges in this case, neither he nor any of the other judges addressed the nature of confidential information in their reasoning.

For example, La Forest J. concluded that unjust enrichment had occurred and that a constructive trust was an appropriate remedy. However, he added that since “it is not the recognition of a right of property that leads to a constructive trust, it is not necessary, therefore, to determine whether confidential information is property.”¹⁵⁴ Sopinka J., on the other hand, arrived at the opposite conclusion of La Forest J. and opposed the remedy of a constructive trust on the basis that this remedy is usually reserved for situations where a right of property is recognized. Most important, he noted that “although confidential information has some of the characteristics of property, its foothold as such is tenuous,”¹⁵⁵ since the originator of an idea does not receive proprietary rights equivalent to those of a patentee.¹⁵⁶ Furthermore, acquisition of the land at issue resulted from the use of information that was both public and private. Since it would be

¹⁵³ At para 25, Sopinka J. in dissent (with McIntyre and Wilson JJ. concurring in part) asserted that a fiduciary relationship is rarely found in the context of commercial transactions, on the basis that the parties have the opportunity to prescribe their own mutual obligations. If Corona, a junior mining company, was in a vulnerable position, this situation occurred not because LAC was a senior mining company but because Corona failed to seek an undertaking from LAC that it would not unilaterally acquire the land at issue. This case thus lacked the dependency or vulnerability which is essential to a finding of a fiduciary relationship.

However, La Forest J. (with Wilson and Lamer JJ. concurring in part) disagreed with Sopinka J.’s reasoning with respect to the finding of a fiduciary relationship. Corona was a junior mining company that needed to raise funds in order to finance the development of its land, which is why it had welcomed the overture of LAC, a senior mining company that had the ability to provide those funds. Since fiduciary obligations can arise out of the specific circumstances of a relationship, La Forest J. concluded that Corona was vulnerable to LAC, such that LAC had a fiduciary obligation to not act to the detriment of Corona’s interests by acquiring the property using confidential information obtained during the negotiation process. La Forest J. also dismissed the notion that the failure to conclude a confidentiality agreement should result in the denial of a fiduciary obligation since “certainty in commercial law, is no doubt, an important value, but it is not the only value,” and “it is simply not the case that business and accepted morality are mutually exclusive domains.”

¹⁵⁴ *LAC Minerals*, *supra* note 71, per La Forest J. at para 76.

¹⁵⁵ *Ibid*, per Sopinka J. at para 172.

¹⁵⁶ *Ibid*, citing *Nichrotherm Electrical Co v Percy*, [1957] RPC 207 at 209.

impossible to assess the role of either type of information, Sopinka J. argued that there was no factual basis for assuming that, but for the confidential information LAC received from Corona, LAC would not likely have acquired the land. Sopinka J. concluded that an award of damages was appropriate.

The *LAC Minerals* case demonstrates that, in an action for breach of confidence, the subject of judicial focus is the *relationship* of confidence, in which confidential information is merely viewed as a “medium” that creates the relationship.¹⁵⁷ Since the characterization of this medium is evidently considered to be of secondary importance, *LAC Minerals* thus offers limited judicial guidance on the nature of confidential information. La Forest J. expressly declined to determine whether confidential information constitutes property. Sopinka J. also refuted the notion of confidential information as property in order to support his assertion that a constructive trust was not an appropriate remedy, but he did not undertake a comprehensive exploration of the nature of confidential information. Instead, he merely voiced his doubts on the characterization of property rights in confidential information in the context of his choice of remedy. Therefore, based solely on Sopinka J.’s statements in *LAC Minerals*, one might conclude that confidential information *likely* does not constitute property.

In any event, it is clear that Canadian judges disagree on the proper characterization of confidential information. Prior to the decision in *LAC Minerals*, Cory J.A. of the Ontario Court of Appeal once offered the following justification for

¹⁵⁷ See Francis Gurry, *Breach of Confidence* (Oxford: Clarendon Press, 1984) at 161-162, cited in *Lac Minerals*, *ibid* at para 42. According to Gurry:

the court’s concern is for the protection of a confidence which *has been created* by the disclosure of confidential information by the confider to the confidant. The court’s attention is thus focused on the protection of the confidential information because it has been the medium for the creation of a relationship of confidence; its attention is *not* focused on the information as a medium by which a *pre-existing* duty is breached [emphases in original].

maintaining confidentiality of information pertaining to commercial enterprises:

Information and its collection, collation and interpretation are vital to most modern commercial enterprises. Compilations of information are often of such importance to the business community that they are securely kept to ensure their confidentiality. The collated, confidential information may be found in many forms covering a wide variety of topics. It may include: painstakingly-prepared computer programs pertaining to all aspects of the firm's business; meticulously-indexed lists of suppliers, with comments as to their efficiency, reliability and time required for delivery; laboriously-compiled lists of customers and their needs; instructions as to manufacturing processes learned from months of experimentation and trial; or lists of employees, including reference to their physical well-being and disciplinary history, that may be required to be kept confidential in compliance with the terms of a collective bargaining agreement. For many businessmen their confidential lists may well be the most valuable asset of their company. Their security will be of utmost importance to the firm.¹⁵⁸

Cory J.A.'s comments emphasize the value of certain business information and the subsequent importance of maintaining the secrecy of business information. In addition to its direct influence on the performance and effective management of a firm, confidential information is often gathered through labour-intensive activities. Because of the effort required to obtain these informational "assets," Cory J.A. advocated for the recognition of confidential business information as property and its subsequent protection as such. He asserted:

If questioned, a businessman would unhesitatingly state that the confidential lists were the "property" of his firm. If they were surreptitiously copied by a competitor or outsider, he would consider his confidential data to have been stolen. The importance of confidential information will increase with the growth of high technology industry. Its protection will be of paramount concern to members of industry and the public as a whole.¹⁵⁹

While Cory J.A. acknowledged that *mere* information may not constitute property, he maintained that there is a right of property in *confidential* information.¹⁶⁰ Moreover, by asserting that confidential business lists can constitute literary works,

¹⁵⁸ *R v Stewart*, (1983) 149 DLR (3d) 583, 42 OR (2d) 225 (ONCA) at para 52 [*Stewart ONCA*].

¹⁵⁹ *Ibid* at para 53.

¹⁶⁰ *Ibid* at para 56.

which are subject to copyright¹⁶¹ that is a “form of property analogous to personal property,”¹⁶² Cory J.A. thereby introduced the possibility that intellectual property protection could encompass confidential business information.

However, although Cory J.A. offered a decisive articulation regarding the nature of confidential information, his statements do not represent the final word on this matter because the judgment of the Ontario Court of Appeal in this case was subsequently overruled by the Supreme Court of Canada.¹⁶³ Furthermore, while the decision of the Supreme Court of Canada in *LAC Minerals* establishes that the protection of confidential information in Canadian law is based upon the duty of confidence, appellate-level judicial guidance on the proper classification of confidential information remains elusive. Nevertheless, Cory J.A.’s comments are noteworthy because they reflect a common philosophical justification for intellectual property protection: based on the notion that “every man is entitled to the fruits of his own labour,” patent and copyright provide safeguards against piracy for the “fruits of labour” of inventors and authors.¹⁶⁴ This perspective also happens to be in accordance with Lord Greene’s reasoning in *Saltman Engineering*, in which a person’s labour with respect to information justified the maintenance of its confidentiality.

Perhaps the notion that people are entitled to the fruits of their labour provides a compelling justification for the right to exclude others from the access and use of information for which one has undertaken painstaking efforts to compile. In other words,

¹⁶¹ *Ibid* at para 67:

Lists compiled for business purposes fall within the term “literary works” and they are a proper subject-matter for copyright.

¹⁶² *Ibid* at para 68.

¹⁶³ See *Stewart* SCC, *supra* note 143.

¹⁶⁴ Harold G Fox, *The Canadian Law of Copyright and Industrial Designs*, 2nd ed (Toronto: Carswell Co, 1967) at 3, cited in *Stewart* ONCA, *supra* note 158 at para 64.

perhaps it is justified for a commercial entity to maintain control over information that it has generated and which is also directly tied to the success of the business. Nevertheless, if such a monopoly over the control of information is warranted, should the right to control information in this manner necessarily endure indefinitely in order to satisfy a person's entitlement to the fruits of his or her labour? In other words, does the right to control information come with a "price" or "trade-off"? These questions will be explored in the following section.

2.1.5. The Nature of Confidential Information: Questions of Balance - The "Bargain" in Intellectual Property Rights Protection

The concept of "entitlement to the fruits of one's labour" is reflected in intellectual property law, but this entitlement does not continue indefinitely. For example, patent¹⁶⁵ and copyright¹⁶⁶ confer monopolies, but the inventions and works to which they pertain face competition in the marketplace following the expiration of the term of protection. There is also a clear public interest aspect to copyright and patent with respect to the dissemination of knowledge. For example, the information contained in a copyrighted work freely circulates among the public even though the author retains exclusive rights to produce, reproduce, or perform the work.¹⁶⁷ Likewise, information

¹⁶⁵ *Patent Act*, supra note 74:

Subject to section 46, where an application for a patent is filed under this Act on or after October 1, 1989, the term limited for the duration of the patent is twenty years from the filing date.

¹⁶⁶ *Copyright Act*, RSC 1985, c C-42, s 6:

The term for which copyright shall subsist shall, except as otherwise expressly provided by this Act, be the life of the author, the remainder of the calendar year in which the author dies, and a period of fifty years following the end of that calendar year.

¹⁶⁷ See *ibid*, s 3(1) for authors' rights with respect to copyrighted works.

about a patent is made publicly available¹⁶⁸ despite the inventor's monopoly on the right to manufacture, sell, and distribute the invention. Figure 1 thus demonstrates the flow of information with respect to the patent process, in which the public is eventually capable of accessing the knowledge associated with a patent. When a patent application is filed with the government, the information is removed from the realm of secrecy and placed within the knowledge of the government. The government maintains the secrecy of patent applications for 18 months and then publicly discloses the information contained therein.¹⁶⁹

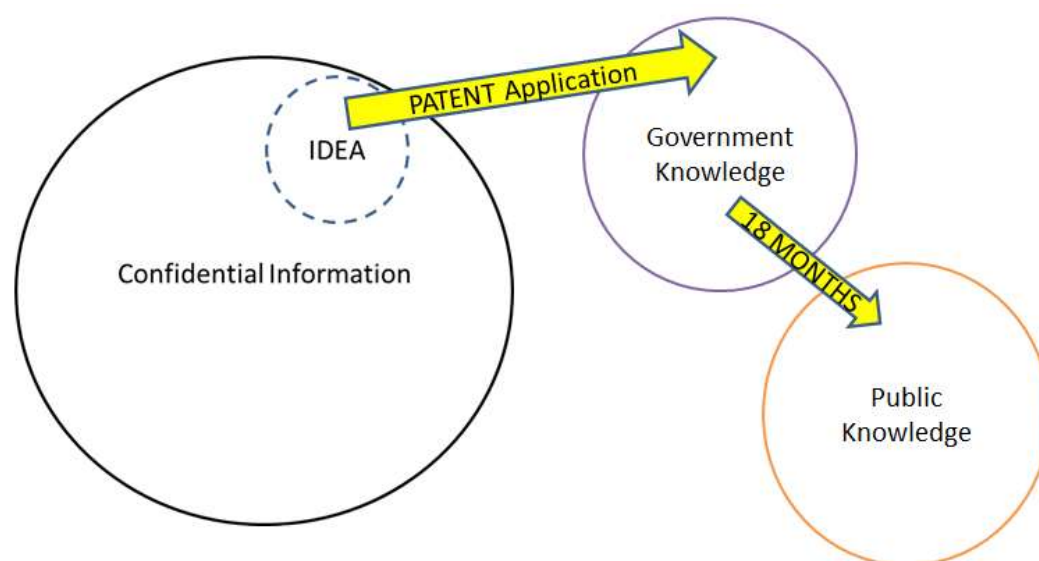


Figure 1 - Flow of Information in the Patent Process

Binnie J. has noted in *Harvard College v. Canada (Commissioner of Patents)*:

¹⁶⁸ *Patent Act*, supra note 74, s 10(1):

Subject to subsections (2) to (6) and section 20, all patents, applications for patents and documents filed in connection with patents or applications for patents shall be open to public inspection at the Patent Office, under such conditions as may be prescribed.

¹⁶⁹ *Ibid*, s 10(2):

Except with the approval of the applicant, an application for a patent, or a document filed in connection with the application, shall not be open to public inspection before a confidentiality period of eighteen months has expired.

...The grant of a patent simply reflects the public interest in promoting disclosure of advancements in learning by rewarding human ingenuity. Innovation is said to be the lifeblood of a modern economy. We neglect rewarding it at our peril. Having disclosed to the public the secrets of how to make or use the invention, the inventor can prevent *unauthorized* people for a limited time from taking a “free ride” in exploiting the information thus disclosed. At the same time, persons skilled in the art of the patent are helped to further advance the frontiers of knowledge by standing on the shoulders of those who have gone before.¹⁷⁰

Binnie J.’s comments with respect to the purpose of patent protection reflect the balance that intellectual property law seeks to achieve between the private interests of innovators and the public interest of society at large. An innovator must be rewarded for the fruits of his or her labour in order to continue to engage in innovation that will ultimately benefit the national economy. Intellectual property protections such as copyright and patent allow the innovator, for a defined period of time, to maintain exclusive rights to the exploitation of creative works or inventions. Public disclosure of information with respect to an invention or creative work, thereby allowing society to benefit from new knowledge contained therein, is accordingly the “price” for a limited-term monopoly.

Ten years after the decision in *LAC Minerals*, the Supreme Court of Canada again had the opportunity to address the nature of confidential information in *Cadbury Schweppes Inc. v. FBI Foods Ltd.*,¹⁷¹ a case concerning the protection of trade secrets. The respondents, Cadbury Schweppes Inc. (“Cadbury Schweppes”) alleged that confidential information regarding their product, Clamato juice, had been used to develop a competing product. Cadbury Schweppes asserted that, where trade secrets constitute the subject matter of wrongful use or disclosure, the policy objectives underlying patent protection are applicable to breaches of confidence in the commercial context.

¹⁷⁰ 2002 SCC 76, [2002] 4 SCR 45 [*Harvard College*].

¹⁷¹ [1999] 1 SCR 142, 167 DLR (4th) 577 [*Cadbury Schweppes*].

Binnie J., writing for the Court, referred to the comments of Lamer J. in *Stewart* in acknowledging that confidential information possesses many characteristics of other forms of property.¹⁷² Nevertheless, he observed that the respondents' characterization of confidential information as property was "controversial," given that an action for breach of confidence has traditionally been "rooted in the relationship of confidence rather than the legal characteristics of the information confided."¹⁷³

Most important, Binnie J. refuted the respondents' arguments that breach of confidence is akin to patent infringement. Binnie J. concluded that the respondents' reliance on intellectual property law ignored the "bargain" that constitutes the heart of patent protection:

A patent is a statutory monopoly which is given in exchange for a full and complete disclosure by the patentee of his or her invention. The disclosure is the essence of the bargain between the patentee, who obtained at the time a 17-year monopoly on exploiting the invention, and the public, which obtains open access to all of the information necessary to practise the invention. Accordingly, at least one of the policy objectives underlying the statutory remedies available to a patent owner is to make disclosure more attractive, and thus hasten the availability of useful knowledge in the public sphere in the public interest... Entrepreneurs in the food industry frequently eschew patent protection in order to avoid disclosure, and thus perhaps perpetuate their competitive advantage beyond the 17-year life span of a patent.¹⁷⁴ We are told that the secrecy of the Coca-Cola recipe has apparently endured for decades. If a court were to award compensation to the respondents on principles analogous to those applicable in a case of patent infringement, the respondents would be obtaining the benefit of patent remedies without establishing that their invention meets the statutory criteria for the issuance of a patent, or paying the price of public disclosure of their secret.¹⁷⁵

Binnie J.'s comments regarding the purpose of patent protection emphasize the key trade-off in intellectual property law, in that the law will provide an innovator with a temporary right to exclude others from exploiting his or her invention or work, so long as

¹⁷² *Ibid* at para 40, citing *Stewart SCC*, *supra* note 170 at 974-975.

¹⁷³ *Ibid* at para 41.

¹⁷⁴ *Ibid* at para 47, citing Hugessen J.A. in *Smith, Kline & French Laboratories Ltd v Canada (Attorney General)*, [1987] 2 FC 359 (FCA) at 366.

¹⁷⁵ *Ibid*.

the rights holder makes the secret therein publicly available. It would appear, then, that contribution to the public interest is a key requisite in the conferral of intellectual property rights.

2.1.6. The Nature of Confidential Information: Confidential Information as (Intellectual) Property - Is the Bargain Present?

In *Cadbury Schweppes*, Binnie J.'s insight into the relevance of intellectual property law with respect to breach of confidence may explain why the respondents were not entitled to receive compensation equivalent to "patent remedies." Nevertheless, these statements focus on the *maintenance of secrecy* of the information and the subsequent lack of a public interest component, rather than the nature of the confidential information at issue. Despite the fact that Binnie J. earlier stated that "the nature of the information may influence the appropriate remedy,"¹⁷⁶ he only acknowledged the controversy surrounding the characterization of confidential information and did not elucidate his own thoughts on the matter.

Similar to the situation in *LAC Minerals*, judicial determination of the nature of confidential information did not occur in *Cadbury Schweppes*, because this appeal focused on the determination of the appropriate remedy. In this context, Binnie J. asserted that a proprietary remedy should not automatically follow for breach of confidence, and that determination of the remedy should depend on a "case-by-case balancing of the equities."¹⁷⁷ The remedy awarded in *LAC Minerals* was driven by "the course of events

¹⁷⁶ *Ibid* at para 43.

¹⁷⁷ *Ibid* at para 48. The Court also noted that in some cases, the relevance of the nature of the information to the choice of remedy will not lie in the information's property status but in its commercial value. In other

that would have likely occurred “but for” the breach,” rather than the “property status” of the confidence.¹⁷⁸ The decision in *Cadbury Schweppes* thus did not settle the law regarding the nature of confidential information.

Nevertheless, *Cadbury Schweppes* does raise an important question with respect to the intellectual property protection of confidential information. As noted by Binnie J. in his observations about the bargain in intellectual property law, innovators in the food industry often avoid patent protection, presumably to maintain secrecy of information that in turn facilitates a competitive edge beyond the life of a patent. Figure 2 illustrates the fact that there is no flow of information with respect to confidential information and the public, such that confidential information has the potential to remain forever excluded from public knowledge (thus the two separate circles in the diagram). The entity in possession of confidential information would thus have a monopoly in the market for the product or service to which the information pertains.

cases, the choice of remedy will be influenced by the “course of events that would likely have occurred but for the breach,” instead of the “property” status of the confidence.

¹⁷⁸ *Ibid.*

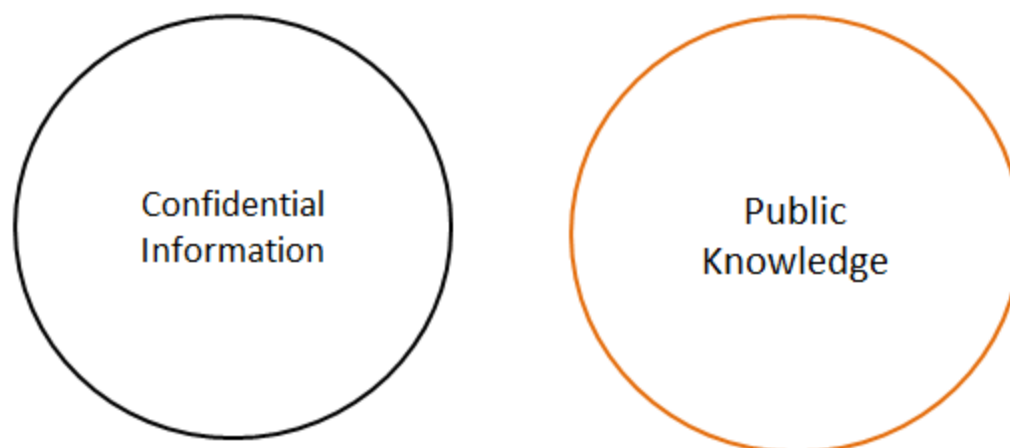


Figure 2 - Relationship between Confidential Information and Public Knowledge - Two Solitudes

Wilkinson notes that, in the context of the current Canadian law, there are three factors that set the protection of confidential information apart from traditional intellectual property devices. Unlike patent or copyright, the protection of confidential information: a) is a product of judicial decision rather than statute; b) is an “unbounded monopoly” that can persist forever, provided that the conditions of confidentiality are maintained; and c) lacks an apparent element of direct public interest, other than the public’s general interest in the success of the national economy.¹⁷⁹ If disclosure of information to benefit the public is the “price” for a limited-term monopoly in exploiting an invention or work, then this bargain appears to be absent in the context of the intellectual property protection of confidential information.

One could argue that subjecting confidential information to intellectual property protection is philosophically justified on the basis that the information is a product of

¹⁷⁹ Wilkinson, “Confidential Information,” *supra* note 49 at 278.

human ingenuity and labour,¹⁸⁰ and lack of protection in this manner would allow others to unjustly avoid the effort and expense of undertaking the same process. Classifying confidential information as “a product of the mind” that warrants the appropriate intellectual property protection would appear to be consistent with the judicial reasoning in the *Coco* and *Saltman Engineering* cases, as well as the underlying rationale of intellectual property law in providing incentives for innovation.

The shift of confidential information protection into the realm of intellectual property law has also brought confidential information into that of international trade. For example, TRIPS articulates the obligations of member states to protect confidential information as follows:

Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- (b) has commercial value because it is secret; and
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.¹⁸¹

NAFTA also mandates the protection of confidential information but, unlike TRIPS, expressly refers to “trade secrets”:

1. Each Party shall provide the legal means for any person to prevent trade secrets from being disclosed to, acquired by, or used by others without the consent of the person lawfully in control of the information in a manner contrary to honest commercial practices, in so far as:

¹⁸⁰ See *TRIPS*, *supra* note 52, art 39(3) and *NAFTA*, *supra* note 51, art 1711(5): For example, in order to merit protection against “disclosure” and “unfair commercial use,” confidential information must have originated from “considerable effort.”

¹⁸¹ *TRIPS*, *ibid*, art 39(2).

(a) the information is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons that normally deal with the kind of information in question;

(b) the information has actual or potential commercial value because it is secret; and

(c) the person lawfully in control of the information has taken reasonable steps under the circumstances to keep it secret.

2. A Party may require that to qualify for protection a trade secret must be evidenced in documents, electronic or magnetic means, optical discs, microfilms, films or other similar instruments.

3. No Party may limit the duration of protection for trade secrets, so long as the conditions in paragraph 1 exist.

4. No Party may discourage or impede the voluntary licensing of trade secrets by imposing excessive or discriminatory conditions on such licenses or conditions that dilute the value of the trade secrets.¹⁸²

Based on the language in the above provisions of TRIPS and NAFTA, one can observe that confidential information derives its value from the very fact that it is secret. Making the information publicly available in accordance with the principles of the traditional “bargain” in intellectual property law would thus destroy this value. Nevertheless, if a purpose of intellectual property protection is to maintain a balance between private and public interests, there should arguably be an exchange between the innovator and the public in accordance with this principle. The act of sequestering knowledge from public scrutiny, particularly when this information could promote scientific or social progress, leads to philosophical difficulties in justifying a monopoly on control over information that will contribute to a perpetual competitive advantage for the entity that controls the information.

¹⁸² NAFTA, *supra* note 51, art 1711.

2.1.7. The Nature of Confidential Information: Controlling Confidential Information - The Tension between Access and Secrecy

Although the value of confidential information and intellectual property rights lies in the rights holder's ability to exclude others from exploiting them, private rights regarding information may conflict with the federal *Access Act*.¹⁸³ The *Access Act* is based on the principles that government information should be available to the public, exceptions to the right of access should be limited and specific, and decisions regarding disclosure of government information should be reviewed independently of the government.¹⁸⁴ Under the *Access Act*, Canadian citizens and permanent residents of Canada are entitled, in accordance with section 4(1), to access any records under the control of a government institution.¹⁸⁵

Despite this entitlement to information in the hands of the government, there are some notable exceptions to disclosure under the *Access Act*.¹⁸⁶ The head of a government institution *must* refuse to disclose any record that contains information that falls within the scope of the exemptions.¹⁸⁷ For example, personal information constitutes one exception to disclosure¹⁸⁸ unless the individual has consented to disclosure, the

¹⁸³ *Access Act*, *supra* note 97.

¹⁸⁴ *Ibid*, s 2(1).

¹⁸⁵ *Ibid*, s 4(1):

Subject to this Act, but notwithstanding any other Act of Parliament, every person who is
 (a) a Canadian citizen, or
 (b) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, has a right to and shall, on request, be given access to any record under the control of a government institution.

¹⁸⁶ These exemptions include broad categories entitled "Responsibilities of Government," "Personal Information," "Third Party Information," "Operations of Government," "Statutory Prohibitions," and "Refusal of Access (where information will be published by a government institution)." This thesis focuses on the category of "Third Party Information."

¹⁸⁷ For example, see *Access Act*, *supra* note 97, ss 19-20.

¹⁸⁸ *Ibid*, s 19(1):

Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in section 3 of the *Privacy Act*.

information is publicly available, or if disclosure is authorized under the *Privacy Act*.¹⁸⁹

Third party information, which encompasses confidential information when placed in the hands of a government organization, constitutes another exception to disclosure and is protected under section 20(1) of the *Access Act*. The provision reads:

Subject to this section, the head of a government institution shall refuse to disclose any record requested under this Act that contains

- (a) trade secrets of a third party;
- (b) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party;
- (b.1) information that is supplied in confidence to a government institution by a third party for the preparation, maintenance, testing or implementation by the government institution of emergency management plans within the meaning of section 2 of the *Emergency Management Act* and that concerns the vulnerability of the third party's buildings or other structures, its networks or systems, including its computer or communications networks or systems, or the methods used to protect any of those buildings, structures, networks or systems;
- (c) information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party; or
- (d) information the disclosure of which could reasonably be expected to interfere with contractual or other negotiations of a third party.¹⁹⁰

The *Access Act* thus attempts to strike a balance between the need to maintain confidentiality of valuable business information and the public interest in the free flow of information. In this context, Figure 3 illustrates the effect of an access request on the flow of information, in which third party information is exempted from disclosure in this manner and thus remains inaccessible by the requester.

¹⁸⁹ *Ibid*, s 19(2):

The head of a government institution may disclose any record requested under this Act that contains personal information if

- (a) the individual to whom it relates consents to the disclosure;
- (b) the information is publicly available; or
- (c) the disclosure is in accordance with section 8 of the *Privacy Act*.

See also, *Privacy Act*, *supra* note 95.

¹⁹⁰ *Access Act*, *ibid*, s 20(1).

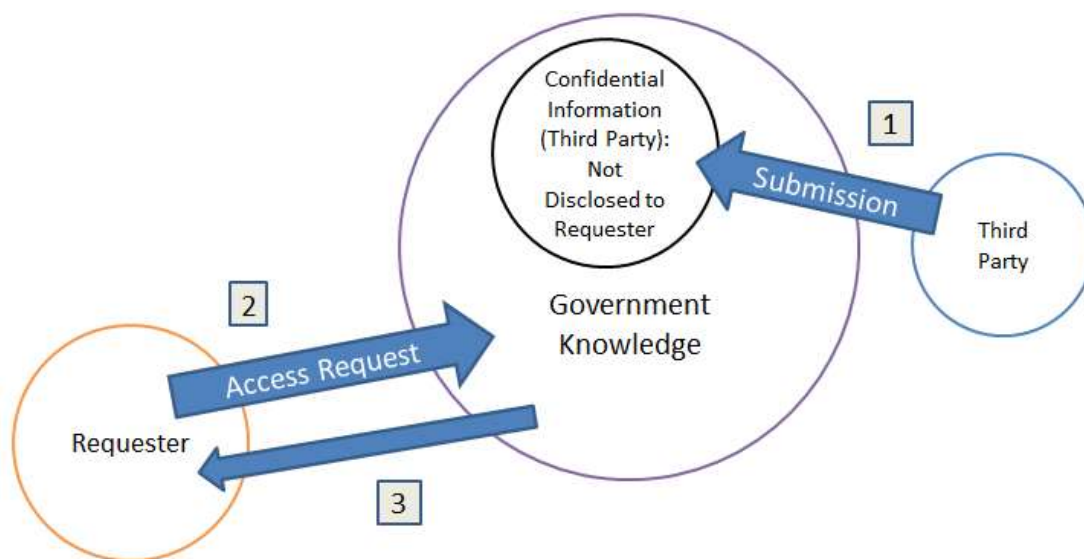


Figure 3 - Flow of Information when Access Request is made

The exceptions to disclosure under the *Access Act* reflect the importance of considering the different and potentially conflicting interests with respect to a particular set of information. In *Stewart*, Lamer J. advocated for a balanced approach with respect to access to information:

Indeed, the realm of information must be approached in a comprehensive way, taking into account the competing interests in the free flow of information and in one’s right to confidentiality or again, one’s economic interests in certain kinds of information.¹⁹¹

Public access to information can “increase transparency in government, contribute to an informed public, and enhance an open and democratic society.”¹⁹² In this way, certain types of information are entitled to confidentiality in order to avoid undermining the very principles of access and promote good governance.¹⁹³ In addition to the exception to the general disclosure requirement, the *Access Act* also provides for

¹⁹¹ *Stewart* SCC, *supra* note 143 at para 32.

¹⁹² *Ontario (Public Safety and Security) v Criminal Lawyers’ Association*, 2010 SCC 23, [2010] 1 SCR 815 at para 1.

¹⁹³ *Ibid.*

procedural protections for third parties where a head of a government institution intends to disclose a record but has reason to believe that the record contains trade secrets or other forms of confidential business information. In this case, the head of an institution is required to give written notice to the third party regarding the access request and the head's intention to disclose the information,¹⁹⁴ thereby allowing the third party to subsequently make representations as to why the record should not be disclosed.¹⁹⁵ It is thus a matter of balancing the tension between the access and secrecy of information in order to satisfy the needs and interests of all the stakeholders involved.

2.1.8 The Nature of Confidential Information: Confidential Information is a Wider Class of Information than Trade Secrets

In the 2012 case, *Merck Frosst Canada Ltd. v. Canada (Minister of Health)* (“*Merck Frosst*”)¹⁹⁶ Cromwell J., writing for the majority, observed that there are different types of confidential information. Cromwell J. first noted the deliberate separation of trade secrets and confidential commercial information under the *Access Act* into exemptions under sections 20(1)(a) and 20(1)(b), respectively. According to Cromwell J., this distinction suggests that the information covered under section 20(1)(b)

¹⁹⁴ *Access Act*, *supra* note 97, s 27(1):

If the head of a government institution intends to disclose a record requested under this Act that contains or that the head has reason to believe might contain trade secrets of a third party, information described in paragraph 20(1)(b) or (b.1) that was supplied by a third party, or information the disclosure of which the head can reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party, the head shall make every reasonable effort to give the third party written notice of the request and of the head's intention to disclose within 30 days after the request is received.

¹⁹⁵ *Ibid*, s 28(1)(a):

Where a notice is given by the head of a government institution under subsection 27(1) to a third party in respect of a record or a part thereof, (a) the third party shall, within twenty days after the notice is given, be given the opportunity to make representations to the head of the institution as to why the record or the part thereof should not be disclosed.

¹⁹⁶ *Merck Frosst SCC*, *supra* note 111.

constitutes a “more general class of confidential, commercial, scientific, and technical information” than the “narrower concept” of “trade secrets” in section 20(1)(a).¹⁹⁷

Cromwell J. further noted that the section 20(1)(a) exemption under the *Access Act* is not subject to disclosure in the public interest, whereas the section 20(1)(b) exemption for confidential information is subject to this type of disclosure.¹⁹⁸

It therefore follows that trade secrets constitute a smaller subset of confidential information. One academic has noted that although all trade secrets are confidential information, not all confidential information constitutes a trade secret.¹⁹⁹ Whether or not a particular set of information constitutes a trade secret will be a question of fact, in which the plaintiff must demonstrate the confidential nature of the information.²⁰⁰

Cromwell J. noted that information does not require an “inherent value” in order to constitute financial, commercial, scientific, or technical information.²⁰¹ Unlike a trade secret, the value of confidential information may fluctuate over time, since it will ultimately depend upon “the use that may be made of it” and “who may want it, and for

¹⁹⁷ *Ibid* at para 106.

¹⁹⁸ *Ibid*.

¹⁹⁹ Stephen D Burns, Todd Newhook & Sebastien A Glittens, “Confidential Information and Governments: Balancing the Public’s Right to Access Government Records and an Oil and Gas Company’s Right to Protect its Confidential Information” (2014) 37 *Dalhousie LJ* 119 at 122.

²⁰⁰ *Ibid* at 124-125. The authors cite *Software Solutions Associates Inc v Depow*, (1989) 15 ACWS (3d) 298 at para 71 in determining whether information constitutes a trade secret. Although these criteria arise in the context of determining what constitutes trade secrets in computer technology, they nonetheless emphasize that the value of a trade secret lies in its secrecy: “(1) The information must not be of a general nature, but rather must be specific; (2) The owner of the trade secret must, at all times, treat the information as confidential and it must be clear that the owner regards the information as a secret. For example, if the owner communicates the information, he must do it in such a way as to show his intention to keep it secret. A trade secret should only be communicated to those employees who have a need to know such information. If the trade secret is to be disclosed to a third party, the owner should require such third party not to disclose or use the trade secret in any way not authorized expressly by the owner; (3) It is not necessary that the information be novel or that it be suitable subject matter for patent or copyright protection. It must, however, be information not generally known to the public. However, it may be information that can be acquired from materials available to the public with the expenditure of time and effort.”

²⁰¹ *Merck Frosst SCC*, *supra* note 111 at para 140.

what purposes.”²⁰² Cromwell J. concluded that a trade secret must be given its “traditional legal meaning,” and that information must satisfy the following criteria to constitute a trade secret:

- a) The information must be secret in an absolute or relative sense (it is known by one or a relatively small number of persons);
- b) The possessor of the information must demonstrate that he has acted with the intention to treat the information as secret;
- c) The information must be capable of industrial or commercial application; and
- d) The possessor must have an interest (e.g. an economic interest) worthy of legal protection.²⁰³

The above criteria emphasize the importance of secrecy with respect to the value of a trade secret. One commentator, Aaron Xavier Fellmeth, has observed that a trade secret’s claim to protection rests upon its possessor’s reasonable efforts to keep it secret by refusing to divulge the secret to any party who does not owe an obligation of confidentiality to the owner.²⁰⁴ Fellmeth further notes that the law of trade secrets protects information that is valuable by virtue of being publicly unknown, such that public knowledge of a trade secret would diminish or destroy whatever monopoly the trade secret confers upon its owner.²⁰⁵

In addition, Cromwell J.’s articulation of a trade secret considers the inherent value of the information and the specificity of its application. Gregory Hagen et al also agree that trade secrets are a subset of the more “inclusive” category of confidential information and tend to be more specific than confidential information: for example, “trade secrets” are typically secret plans, processes or formulae, and compounds, recipes,

²⁰² *Ibid* at para 140, citing *Air Atonabee Ltd v Canada (Minister of Transport)*, (1989) 27 FTR 194, 27 CPR (3d) 180 at 267.

²⁰³ *Ibid* at para 109, citing *Astrazeneca Canada Inc v Health Canada*, 2005 FC 189, 275 FTR 133 at para 64.

²⁰⁴ Aaron Xavier Fellmeth, “Secrecy, Monopoly, and Access to Pharmaceuticals in International Trade Law: Protection of Marketing Approval Data under the TRIPS Agreement” (2004) 45 *Harvard Int’l L J* 443 at 463 [Fellmeth].

²⁰⁵ *Ibid* at 462.

or tools, whereas confidential information can include customer lists, knowledge or opportunities, “and just about any information that is of value when confidential to the holder.”²⁰⁶

The characterization of trade secrets as a narrower class of confidential information is further supported by section 20(6) of the *Access Act*, which authorizes disclosure in the public interest. While *all* confidential information constitutes an exception to the general requirements of disclosure under section 4(1) of the *Access Act*, there is an “exception to the exception,” in which *some* types of confidential information can be subject to disclosure:

The head of a government institution **may** disclose all or part of a record requested under this Act that contains **information described in any of paragraphs (1)(b) to (d)** if

- (a) the disclosure would be in the **public interest** as it relates to public health, public safety or protection of the environment; **and**
- (b) the **public interest in disclosure clearly outweighs in importance** any financial loss or gain to a third party, any prejudice to the security of its structures, networks or systems, any prejudice to its competitive position or any interference with its contractual or other negotiations [emphases added].²⁰⁷

Provisions authorizing the disclosure of confidential information for the purposes of protecting public health or the public interest can also be found in other Canadian legislation. For instance, where there is a “serious risk of injury to human health,” section 21.1 of the federal *Food and Drugs Act* states that the Minister of Health “may disclose confidential business information about a therapeutic product” without the consent of the person to whose business the information relates.²⁰⁸ Similarly, the

²⁰⁶ Hagen et al, *supra* note 68 at 575.

²⁰⁷ *Access Act*, *supra* note 97, s 20(6).

²⁰⁸ *Food and Drugs Act*, RSC, 1985, c F-27, s 21.1(2):

The Minister may disclose confidential business information about a therapeutic product without notifying the person to whose business or affairs the information relates or

Minister of Health may disclose confidential business information about a therapeutic product to the government, an advisor to the Minister, or someone who carries out functions that are related to the “protection or promotion of human health or the safety of the public.”²⁰⁹ The *Food and Drugs Act* defines “confidential business information” as business information that has “actual or potential economic value” and that is not publicly available, in which measures have been taken to ensure that the information remains not publicly available.²¹⁰ A “therapeutic product” is defined as “a drug or device or any combination of drugs and devices.”²¹¹ Thus, the *Food and Drugs Act* indicates that the confidential information generated for drugs in clinical trials does not constitute a trade secret.

Although the Supreme Court of Canada has ultimately declined to comment on the nature of confidential information, the tension between protecting confidential

obtaining their consent, if the Minister believes that the product may present a serious risk of injury to human health.

²⁰⁹ *Ibid.*, s 21.1(3):

The Minister may disclose confidential business information about a therapeutic product without notifying the person to whose business or affairs the information relates or obtaining their consent, if the purpose of the disclosure is related to the protection or promotion of human health or the safety of the public and the disclosure is to

(a) a government;

(b) a person from whom the Minister seeks advice; or

(c) a person who carries out functions relating to the protection or promotion of human health or the safety of the public [emphasis added].

²¹⁰ *Ibid.*, s 2:

confidential business information, in respect of a person to whose business or affairs the information relates, means — subject to the regulations — business information

(a) that is not publicly available,

(b) in respect of which the person has taken measures that are reasonable in the circumstances to ensure that it remains not publicly available, and

(c) that has actual or potential economic value to the person or their competitors because it is not publicly available and its disclosure would result in a material financial loss to the person or a material financial gain to their competitors [emphasis in original].

²¹¹ *Ibid.*:

therapeutic product means a drug or device or any combination of drugs and devices, but does not include a *natural health product* within the meaning of the *Natural Health Products Regulations* [emphasis in original].

information and sharing it for the greater public good is reflected in the comments made by Lamer J. in *Stewart*:

From a social point of view, whether confidential information should be protected requires a weighing of interests much broader than those of the parties involved. As opposed to the alleged owner of the information, society's best advantage may well be to favour the free flow of information and greater accessibility by all. Would society be willing to prosecute the person who discloses to the public a cure for cancer, although its discoverer wanted to keep it confidential?²¹²

Lamer J. thus seems to suggest that in some contexts, it may not be clear as to who should hold the right to control a particular set of information. In creating valuable information, it follows that the generating entity should be granted the right to control this information. However, if that entity's rights of control unduly restrict the free flow of information, especially when disclosure of this information can save human lives, perhaps these rights should be limited for the benefit of the public at large. The need to acknowledge other legitimate claims to the same set of information accordingly calls into question the theoretical validity of the *permanent* secrecy of confidential information.

Nevertheless, despite providing for disclosure of confidential information in the public interest, section 21.1 of the *Food and Drugs Act* and section 20(6) of the *Access Act* do not mandate disclosure, but instead leave the decision of disclosure to the discretion of the institutional head.²¹³ Most important, Hagen et al further note that in Canada, there is currently no difference in juridical treatment as between trade secrets and confidential information.²¹⁴ Therefore, there is no time limit on the protection of

²¹² *Stewart SCC*, *supra* note 143 at para 28.

²¹³ For example, the *Access Act*, *supra* note 97, s 20(6) states that the head of a government institution "may" disclose all or part of a record containing confidential information. The use of the word "may" indicates that the government head is permitted, not mandated, to disclose the information: see *Interpretation Act*, RSC, 1985, c I-21, s 11: "The expression "shall" is to be construed as imperative and the expression "may" as permissive."

²¹⁴ Hagen et al, *supra* note 68 at 575.

secrets, and obligations of confidence may be claimed and enforced as long as the information is kept secret.²¹⁵ The strategy of keeping information a secret is an effective and flexible way to maintain a competitive advantage in light of changing business practices and technology: legal protection of secrets allows an idea, information, process, or technology to be tested without fear of appropriation, thereby encouraging investment.²¹⁶ Moreover, Hagen et al assert that the legal protection of confidential information also fosters ethical behaviour in fair competition by “promoting, protecting, and enforcing relationships founded on trust and confidence.”²¹⁷

2.1.9. Conclusion on the Nature of Confidential Information

While legal scholars such as Weinrib and Cory J.A. have explored the notion of confidential information as property, the law of confidential information in Canada does *not* characterize confidential as property. As demonstrated in cases such as *LAC Minerals* and *Cadbury Schweppes*, the protection of confidential information in Canada is based upon the duty of confidence, in which a breach of confidence will give rise to a cause of action. Although confidential information may continue to be discussed in terms of property because of its classification as *intellectual* property under international trade agreements, confidential information differs from traditional intellectual property devices such as copyright and patent because it lacks a public interest component that would justify its continued secrecy and a subsequent limitless monopoly.

²¹⁵ *Ibid.*

²¹⁶ *Ibid.* The authors note that, while an idea may not be sufficiently novel to satisfy the requirements for a patent, secrecy can be used to “develop technology, a business method, a mining claim, or a recipe for a juice mix,” and this knowledge can be shared among a small group of confidantes in order to foster its development or implementation.

²¹⁷ *Ibid.*

Therefore, it is perhaps more useful to frame a discussion of the protection of confidential information in terms of a party's rights of control over information, as this framework also considers the possibility that there may be multiple, yet also compelling claims to the same set of confidential information. As this thesis will show, the existence of potentially conflicting rights to information is particularly salient in the pharmaceutical context.

2.2. Regulation of the Drug Approval Process: Protecting Public Health

The ultimate goal of national regulatory authorities, such as Health Canada, is to protect and promote public health.²¹⁸ Governments have a responsibility to protect their citizens, especially in areas where citizens are not able to protect themselves.²¹⁹

Government regulation and oversight is particularly necessary with respect to the manufacture and sale of pharmaceutical products. Drugs are not ordinary consumer goods, since most consumers do not possess the requisite knowledge to make informed decisions “about when to use drugs, which drugs to use, how to use them, and to weigh potential benefits against risks.”²²⁰ Although medical doctors are presumably competent to diagnose a patient's disease and select the appropriate course of treatment, a comprehensive understanding of the complex scientific issues that are associated with medicines often requires highly specialized training in the field of clinical pharmacology.²²¹ It is thus in the public interest to have a strong, centralized regulator

²¹⁸ Rago & Santoso, *supra* note 10 at 67.

²¹⁹ *Ibid.*

²²⁰ *Ibid.*

²²¹ *Ibid.*

that has both the knowledge and authority to make definitive judgments on the safety, efficacy, and labelling of medicines.²²²

Another important purpose of a national regulatory agency is to provide a check on powerful pharmaceutical companies that might allow commercial interests to prevail over public safety. A regulator's failure to uphold its responsibility regarding adequate oversight within its authority can lead to disastrous consequences for public health. For example, in 1999, the pharmaceutical company Merck & Co., Inc. ("Merck") was granted approval for the drug rofecoxib (also known as Vioxx) by the Food and Drug Administration (FDA), the national health regulator in the U.S.²²³ On September 30, 2004, after more than 80 million patients had taken rofecoxib and annual sales had reached \$2.5 billion, Merck withdrew rofecoxib from the market owing to increased risks for myocardial infarctions and stroke. One commentator, Eric Topol, has noted that Merck could have conducted a specific trial to ascertain cardiovascular risks and benefits, but such a trial was never conducted even though the FDA possessed the authority to mandate one.²²⁴ Merck instead issued a "relentless series of publications" that asserted the safety of rofecoxib, which were subsequently complemented by papers in peer-reviewed medical literature by Merck employees and consultants.²²⁵ Merck also spent over \$100 million per year in direct-to-consumer advertising, another activity regulated by the FDA, which was essential in generating its massive annual sales for rofecoxib.²²⁶ Despite the efforts of many investigators in conducting and publishing independent

²²² Erika Lietzan, "A New Framework for Assessing Clinical Trial Data Transparency Initiatives" (2014) 18 Marq Intell Prop L Rev 33 at 78 [Lietzan, "Transparency Initiatives"].

²²³ Eric J Topol, "Failing the Public Health – Rofecoxib, Merck, and the FDA" (2004) New Eng J Med 351 at 1707 at 1707.

²²⁴ *Ibid.*

²²⁵ *Ibid.*

²²⁶ *Ibid.*

research on the cardiovascular toxicity of rofecoxib, only the FDA was authorized to take action regarding the findings.²²⁷ In estimating that there may be “tens of thousands of patients who have had major adverse events attributable to rofecoxib,” Topol thus asserts that the FDA failed to fulfil its responsibilities to the public by passively waiting for data to accrue and in failing to exercise its regulatory power.²²⁸

Effective regulatory systems clearly require appropriate action on the part of the people who run them, particularly when these individuals are the only ones authorized to act. Since the efficacy of regulatory systems depends on the actual enforcement of the laws therein by individuals, the system may not always ensure perfect safeguards against cases such as the rofecoxib incident. However, this reality does not detract from the necessity of legislative requirements that mandate standards for rigorous scientific testing of new compounds in preparation for their subsequent use by humans. This process involves the balancing of the benefits, risks, and the availability of other drugs for a particular disease.²²⁹ In this way, when Health Canada decides that a drug is safe and effective, this approval means that the drug’s benefits outweigh the risks, which reflects a policy choice based in part on society’s collective level of risk tolerance.²³⁰

As mentioned in Chapter One of this thesis, the manufacturer of a new drug must submit evidence to the government regarding the drug’s safety and efficacy before the drug can be marketed and sold in Canada. In order to receive the NOC that indicates proof of the government’s approval, the manufacturer must first file a New Drug

²²⁷ *Ibid* at 1708.

²²⁸ *Ibid* at 1708.

²²⁹ H Thomas Austern, “Drug Regulation and the Public Health” (1964) 39 NYUL Rev 771 at 776.

²³⁰ Lietzan, “Transparency Initiatives,” *supra* note 222 at 78.

Submission (NDS) with the Minister of Health.²³¹ The NDS must contain “sufficient information and material to enable the Minister to assess the safety and effectiveness of the new drug,” including the following: detailed reports of tests made to establish the drug’s safety under the recommended purpose and conditions of use; “substantial evidence” of the new drug’s clinical effectiveness for the recommended purpose and conditions of use; and details of the tests to control the drug’s potency, purity, safety, and stability.²³²

An NDS consists of a vast amount of information, much of which is generated by clinical trials which are heavily regulated in Canada by the *Food and Drug Regulations*.²³³ Clinical trials typically consist of four phases. During Phase I, an experimental drug is tested on a small group of people for the first time in order to assess the drug’s safety or toxicity, identify side effects, and determine a safe dosage range.²³⁴ In Phase II, the drug is administered to a larger group of 100 or more individuals to further assess the drug’s safety and obtain preliminary data on the drug’s effectiveness for a particular disease or condition.²³⁵ In Phase III, the drug is administered to a group of 1000 or more people to confirm the drug’s effectiveness, monitor side effects, compare the drug to commonly used treatments, and collect information that will allow the drug to

²³¹ *Food and Drug Regulations*, *supra* note 5, s C.08.002(1):

No person shall sell or advertise a new drug unless

(a) the manufacturer of the new drug has filed with the Minister a new drug submission, an extraordinary use new drug submission, an abbreviated new drug submission or an abbreviated extraordinary use new drug submission relating to the new drug that is satisfactory to the Minister;

(b) the Minister has issued, under section C.08.004 or C.08.004.01, a notice of compliance to the manufacturer of the new drug in respect of the submission; and

(c) the notice of compliance in respect of the submission has not been suspended under section C.08.006.

²³² See *ibid*, s C.08.002(2).

²³³ See *ibid*, s C.05.010.

²³⁴ Health Canada, *Clinical Trials and Drug Safety*, May 2013, (accessed April 4, 2017) at 2, online: <http://www.hc-sc.gc.ca/hl-vs/alt_formats/pdf/iyh-vsv/med/clinical_trails-essais_cliniques-eng.pdf>.

²³⁵ *Ibid*.

be used safely.²³⁶ Finally, Phase IV occurs once the drug is approved and is available on the market, and researchers gather information on the drug's optimal use and its long-term benefits and risks.²³⁷ The entities that conduct clinical trials ("clinical trial sponsors")²³⁸ are required to maintain "complete and accurate records" with respect to the use of a drug in a clinical trial and are obligated to identify and subsequently contact clinical trial participants if the sale of the drug may endanger their health or that of other people.²³⁹

The regulatory process for new drugs is particularly relevant to the protection of confidential information in the pharmaceutical context. As will be discussed in the next section of this thesis, information in an NDS is disclosed to the government in the course of the market approval process, but the information constitutes third party information that is generally exempt from disclosure under section 20 of the *Access Act*. Moreover, the pharmaceutical context offers a clear illustration of the struggle between the competing interests of the parties that wish to gain access to confidential information and those that seek to maintain its secrecy.

²³⁶ *Ibid.*

²³⁷ *Ibid.*

²³⁸ *Food and Drug Regulations*, *supra* note 5, s C.05.001:

sponsor means an individual, corporate body, institution or organization that conducts a clinical trial [emphasis in original].

²³⁹ *Ibid.*, s C.05.012(3):

The sponsor shall maintain complete and accurate records in respect of the use of a drug in a clinical trial, including...

(d) records respecting the enrolment of clinical trial subjects, including information sufficient to enable all clinical trial subjects to be identified and contacted in the event that the sale of the drug may endanger the health of the clinical trial subjects or other persons.

2.3. Access and Control over Confidential Information in the Pharmaceutical Context

In section 2.1.8, the 2012 Supreme Court of Canada decision, *Merck Frosst*,²⁴⁰ was discussed as supporting the characterization of trade secrets as a subset of the broader category of confidential information. However, the key role of this decision in the analysis in this thesis concerns the aspect of the case revolving around the protection of confidential information in the pharmaceutical context with respect to exceptions to disclosure under the *Access Act*. The decision demonstrates the tension between access and secrecy: in the *Merck Frosst* case, the access was sought by someone who was not a subject of the data. In this thesis, the access that is of concern is access to the data of a person who is a subject of the data.

Cromwell J., writing for the majority in *Merck Frosst*,²⁴¹ first acknowledged that broad rights of access to government information serve an important public purpose by ensuring accountability, thereby strengthening democracy.²⁴² On the other hand, Cromwell J. noted that providing access to government information also engages the interests of third parties that provide information to the government for regulatory purposes, since the information in question may include trade secrets and “other confidential commercial matters” which may be valuable to competitors of the third party.²⁴³ Since disclosing valuable confidential information may result in financial harm

²⁴⁰ See *Merck Frosst* SCC, *supra* note 111.

²⁴¹ The Court was split 6-3. Deschamps J., in dissent, agreed with Cromwell J. with respect to the issues of notice to third parties and the requirement for third parties to demonstrate, on a balance of probabilities, why disclosure should not be made. However, Deschamps J. asserted that the judgments of the Federal Court, 2006 FC 1200 and 2006 FC 1201, did not contain a “palpable and overriding error that would justify this Court’s intervention” so should be restored: See *Merck Frosst*, *ibid*, per Deschamps J. at paras 243-244.

²⁴² *Merck Frosst* SCC, *supra* note 111, per Cromwell J. at para 1.

²⁴³ *Ibid* at para 2.

to a third party, the routine disclosure of this information may “ultimately discourage research and innovation.”²⁴⁴

The *Merck Frosst* decision thus illustrates the tension between the public’s right to access government information and the need to preserve the private interests of third parties. This decision is the final result of lengthy and complex litigation, in which five decisions led to the appeals before the Supreme Court of Canada. At issue was the information contained in an NDS and Supplementary New Drug Submission (SNDS),²⁴⁵ which had been submitted to the respondent Health Canada by the appellant, Merck Frosst Canada Ltd. (“Merck”), in the course of obtaining regulatory market approval for an asthma medication, Singulair®. The initial judicial review was heard by Harrington J. of the Federal Court in 2004,²⁴⁶ whose decision was subsequently overturned by the Federal Court of Appeal in 2005.²⁴⁷ The matter was returned to the Federal Court, which

²⁴⁴ *Ibid.*

²⁴⁵ A supplement to an NDS is submitted to request authorization to market a drug that has already been approved and for which certain changes have been made. See *Food and Drug Regulations*, *supra* note 5, s C.08.003 (1):

Despite section C.08.002, no person shall sell a new drug in respect of which a notice of compliance has been issued to the manufacturer of that new drug and has not been suspended under section C.08.006, if any of the matters specified in subsection (2) are significantly different from the information or material contained in the new drug submission, extraordinary use new drug submission, abbreviated new drug submission or abbreviated extraordinary use new drug submission, unless

- (a) the manufacturer of the new drug has filed with the Minister a supplement to that submission;
- (b) the Minister has issued a notice of compliance to the manufacturer of the new drug in respect of the supplement; and
- (c) the notice of compliance in respect of the supplement has not been suspended under section C.08.006.

²⁴⁶ *Merck Frosst Canada & Co v Canada (Minister of Health)*, 2004 FC 959, [2005] 1 FCR 587 [*Merck Frosst* FC 2004]. Harrington J. allowed Merck’s application and held that all the information at issue was third party information that would not exist but for Merck’s NDS.

²⁴⁷ *Merck Frosst Canada & Co v Canada (Minister of Health)*, 2005 FCA 215, [2006] 1 FCR 379. Desjardins J.A. of the Federal Court of Appeal held that Harrington J. had erred in law in ruling that the documents in question met the criteria for exemption under paragraph 20(1)(b) of the *Access Act*.

heard the applications for judicial review related to the NDS²⁴⁸ and SNDS.²⁴⁹ For both of the NDS and SNDS judgments, Health Canada appealed and Merck cross-appealed: the Federal Court of Appeal heard the appeals and cross-appeals concurrently and delivered one judgment.²⁵⁰

In accordance with the approval process, Merck had made comprehensive disclosure to Health Canada of all its information on Singulair®, including raw data from pre-clinical and clinical studies.²⁵¹ Figure 4 illustrates the flow of information with respect to the data submitted by Merck. Information in an NDS, such as clinical trial data, is disclosed to the government, and information contained in government records is subject to access requests through the *Access Act*.

²⁴⁸ *Merck Frosst Canada Ltd v Canada (Minister of Health)*, 2006 FC 1201, 158 ACWS (3d) 689. Merck asked that the Federal Court issue a declaratory order regarding the lawfulness of the procedure followed by Health Canada in processing the request for access to information. Merck also asked for an order prohibiting the disclosure of the records at issue. Beaudry J. concluded that disclosure of some of the record without prior notice to Merck contravened the spirit of the *Access Act*, such that Merck was entitled to a declaratory order. However, Beaudry J. found that approximately 65 pages of the record could be disclosed, while over 170 pages were exempt from disclosure.

²⁴⁹ *Merck Frosst Canada Ltd v Canada (Minister of Health)*, 2006 FC 1200, 301 FTR 241. Merck sought an order from the Federal Court declaring illegal the process followed by Health Canada in handling the access to information request and an order prohibiting the disclosure of the documents at issue. Beaudry J. found that Merck was entitled to a declaratory order on the basis that disclosure of some of the record without prior notice to Merck contravened the *Access Act*. However, while almost 60 pages of the record were exempt from disclosure, the remaining pages could be disclosed.

²⁵⁰ *Canada (Health) v Merck Frosst Canada Ltd*, 2009 FCA 166, 400 NR 1 [*Canada v Merck Frosst*]. In allowing the appeals and dismissing the cross-appeals, Desjardins J.A., writing for a unanimous court, found that Beaudry J. had made several legal errors and held that all of the remaining pages at issue with respect to both the NDS and SNDS should be disclosed.

²⁵¹ *Merck Frosst SCC*, *supra* note 111 at para 16, citing Health Canada, *Therapeutic Products Programme Guidelines – Preparation of Human New Drug Submissions*, (1991), available online: <http://publications.gc.ca/collections/collection_2013/sc-hc/H42-2-38-1991-eng.pdf> (accessed April 9, 2017): The preparation of new drug submissions consists of five main parts. Part 5 must contain the raw data from preclinical and clinical studies.

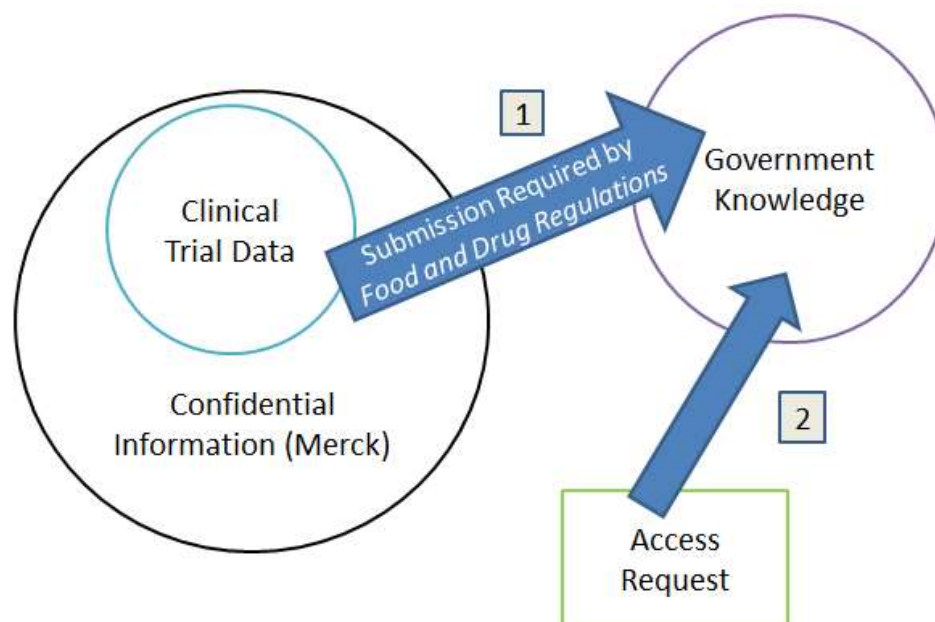


Figure 4 - Flow of Information with respect to Data Submitted by Merck

Health Canada subsequently received access to information requests under the *Access Act* with respect to information contained in Merck’s NDS and SNDS. The specific documents to which the requester²⁵² sought access were the NOC, the Comprehensive Summary,²⁵³ the Health Canada reviewers’ notes,²⁵⁴ and the correspondence²⁵⁵ between Health Canada and Merck. In accordance with procedural

²⁵² The requester is never identified in any of the judgments. However, the comments of Harrington J. of the Federal Court suggest that the access request originated from one of Merck’s competitors: See *Merck Frosst FC 2004*, *supra* note 246 at para 38:

Merck Frosst took issue with the documents which had already been released on the basis that information such as control and file numbers provides valuable and competitive information which is helpful for tracking purposes, and allows the requester to assess the various phases of the review process.

²⁵³ *Merck Frosst SCC*, *supra* note 111 at para 16: The Comprehensive Summary is the “heart” of the NDS and consists of factual, concise descriptions of the methodology, results, conclusions, and evaluations of the clinical studies.

²⁵⁴ *Ibid* at para 17: Once a manufacturer submits all of its information on its new drug, Health Canada reviews and evaluates the information, and the reviewers comment on the provided information.

²⁵⁵ *Ibid*: During the review and evaluation process of a drug, the reviewers often pose questions and seek additional information from the manufacturer. These requests and other communications between Health Canada and the manufacturer thereby constitute “correspondence.”

requirements under the *Access Act*, Health Canada was required to give notice to Merck of the request for access and of Health Canada's intent to disclose part of the NDS record.

While Health Canada found that 30 of the 550 pages identified under the access request contained confidential information and could not be disclosed, Health Canada also concluded that the NDS record contained 15 pages that did not constitute confidential information. Health Canada subsequently disclosed these pages without notifying Merck. In contrast, Merck claimed that *all* of the information covered by the access request, including the disclosed pages, was exempt from disclosure. The same events unfolded with respect to the SNDS, in which Health Canada disclosed eight pages of the SNDS after concluding that they contained no confidential information, while Merck insisted that none of the 300 pages of the SNDS could be disclosed. Thus, Merck complained that Health Canada failed to give Merck notice and an opportunity to make objections before disclosing some of its confidential information and that Health Canada did not conduct a sufficiently detailed review of the documents before deciding the information was subject to disclosure. In addition, Merck claimed that certain categories of records, of which an NDS and a SNDS are part, should "automatically" trigger a right to notice because of the confidentiality and competitive value of the information contained therein.²⁵⁶

Cromwell J. rejected Merck's assertion that the proposed disclosure of any part of an NDS or SNDS automatically triggers a duty to give notice.²⁵⁷ Cromwell J. noted that the ordinary meaning of the notice provision did not support Merck's position of a

²⁵⁶ *Ibid* at para 62.

²⁵⁷ *Ibid* at para 69.

right to notice regarding particular categories of records.²⁵⁸ In addition, Merck’s position was not consistent with an important principle of the *Access Act*, in that exceptions to the right of access should be “limited and specific.”²⁵⁹ The creation of classes of documents that would “presumptively trigger the notice requirement and be presumptively exempt from disclosure” would thus be inconsistent with this principle.²⁶⁰

Nevertheless, Cromwell J. acknowledged that observing a low threshold for triggering the notice requirement would ensure procedural fairness and reduce the risk of the mistaken disclosure of exempted information.²⁶¹ Deschamps J. also raised the question of whether a government entity is capable of determining whether all confidential information has been redacted from a record intended for disclosure.

According to Deschamps J.:

Health Canada’s statement that all confidential information has been redacted is just an argument. It is not proof that all such information has in fact redacted. Indeed, at the beginning of the proceedings, Health Canada took the position that none of the information was confidential. The number of documents that either were subsequently found to be exempt in their entirety or were redacted extensively is a clear indication that Health Canada’s word cannot be taken as proof.²⁶²

²⁵⁸ *Ibid* at para 66, citing *Access Act*, *supra* note 97, s 27(1):

If the head of a government institution intends to disclose a record requested under this Act that contains or that the head has reason to believe might contain trade secrets of a third party, information described in paragraph 20(1) (b) or (b.1) that was supplied by a third party, or information the disclosure of which the head can reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party, the head shall make every reasonable effort to give the third party written notice of the request and of the head’s intention to disclose within 30 days after the request is received.

²⁵⁹ *Ibid* at para 67:

The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.

²⁶⁰ *Ibid*.

²⁶¹ *Ibid* at para 80.

²⁶² *Ibid*, per Deschamps J. at para 258.

Because an institutional head has equally important duties “to disclose and not to disclose,” the institutional head must thus give third parties notice if they are in doubt about whether the information is exempt.²⁶³ In particular, a third party will be in a better position than a head of a government institution to identify information that falls within the exemptions to disclosure under the *Access Act*. A third party will have knowledge and understanding about the industry in which it participates, as well as “intimate knowledge” of the information at issue and the possible harm that could result from its disclosure.²⁶⁴ Therefore, a third party’s assistance will be required “to know how, or if, the third party treated the information as confidential,” such that “whether the information is confidential cannot be determined without representations from the third party.”²⁶⁵

It is important to note that Cromwell J. did not dispute the potential value of Merck’s confidential information. He acknowledged that “disclosure of information that is not already in the public domain and that could give competitors a head start in product development, or which they could use to their competitive advantage, may be shown to give rise to a reasonable expectation of probable harm or prejudice to the third party’s competitive position.”²⁶⁶ Instead, Merck’s claims were dismissed owing to its failure to present sufficient evidence to support its claims under the various exemptions under section 20 of the *Access Act*.

With respect to the section 20(1)(a) exemption for trade secrets, Cromwell J. noted that Merck’s evidence was not capable of establishing that the documents in the

²⁶³ *Ibid*, per Cromwell J. at para 84.

²⁶⁴ *Ibid* at para 79.

²⁶⁵ *Ibid* at para 79, citing Deschamps J. in *HJ Heinz Co of Canada Ltd v Canada (Attorney General)*, 2006 SCC 13, [2006] SCR 441 at para 51.

²⁶⁶ *Ibid* at para 220.

NDS record either contained trade secrets or revealed trade secrets.²⁶⁷ Moreover, to the extent that portions of the records revealed trade secrets, this information had been redacted.²⁶⁸ Merck failed to demonstrate how the remaining information constituted trade secrets within the meaning of the exemption, since “the conclusion that virtually blank pages constituted trade secrets is a palpable and overriding error” on the part of the reviewing judge.²⁶⁹

Merck encountered similar evidentiary problems with respect to the section 20(1)(b) exemption: Merck could not explain why the remaining information on heavily redacted pages constituted confidential information. Merck argued that its assembled list of studies and articles was not public knowledge, and that releasing the articles in response to the access request would link them to Singulair® and the NDS or the SNDS. Cromwell J. concluded that Merck’s evidence failed to support the claim that Merck’s listing of the studies was confidential information, although he did not “foreclose the possibility of a claim of this nature being established in some cases in which the evidence supported it.”²⁷⁰

Finally, Merck argued that the compilation of publicly available studies is a separate work from the studies themselves, a separate work which had been created by Merck’s employees using substantial time and resources. The studies themselves may have been publicly available, but “what was not publicly available...is the way a group of publicly available studies was compiled for a particular purpose.”²⁷¹ In determining

²⁶⁷ *Ibid* at para 120.

²⁶⁸ *Ibid* at para 121.

²⁶⁹ *Ibid* at para 124.

²⁷⁰ *Ibid* at para 182.

²⁷¹ *Ibid* at para 147. Although Merck did not purport to assert a proprietary interest in the information, it is interesting to note that Merck’s arguments nonetheless reflect the notion that people are entitled to the

whether this information could trigger an exemption under section 20(1)(c) with respect to the reasonable expectation of harm to Merck, Cromwell J. agreed that “it may be possible in some cases to show that the way in which publicly available information has been assembled in a particular situation is not, itself, publicly known.”²⁷² Nevertheless, Cromwell J. again noted that Merck failed to show evidence about how disclosure of the redacted form of the information, as presented by Health Canada, would reasonably be expected to give rise to the harm and prejudice claimed by Merck. Furthermore, in light of these redactions, Cromwell J. asserted that the public interest favoured disclosure of the redacted records, noting that “it is particularly important to allow broad access to this sort of information in the context of the pharmaceutical industry...Health Canada systematically posts on its website about undesirable effects of all drugs sold in Canada.”²⁷³

The *Merck Frosst* case illustrates the battle for control over confidential information in the pharmaceutical context. Moreover, since the *Food and Drug Regulations* require drug manufacturers to disclose all information about a new drug to the government, the protection of confidential information in *Merck Frosst* occurred in a statutory context rather than at common law, a statutory context in which the *Access Act* protects third party information through exemptions to disclosure. The *Merck Frosst* case is thus informative with respect to a discussion about data exclusivity, which is also based on a statutory regime.²⁷⁴ Harrington J. of the Federal Court specifically noted that,

fruits of their labour – in this case, the compilation of the studies – which is a notion that has traditionally been used to justify private property rights.

²⁷² *Ibid* at para 210.

²⁷³ *Ibid* at para 225.

²⁷⁴ See *Food and Drug Regulations*, *supra* note 5, s C.08.004.1(1). Canada’s data exclusivity framework under the *Food and Drug Regulations* will be further discussed in Chapter Three.

to recoup their investment in the costly development of new medicines, innovator pharmaceutical companies “are dependent upon patent protection and protection of data submitted to government authorities.”²⁷⁵

However, it is important to note that the *Merck Frosst* decision did not concern data exclusivity at all. The Federal Court of Appeal noted that Merck cited, but ultimately did not argue at trial, Canada’s obligations under TRIPS and NAFTA in support of its position against disclosure under the *Access Act*.²⁷⁶ Although it is not expressly mentioned in any of the judgments, the fact that Merck did not rely on data exclusivity protection in its arguments likely occurred because the term of data exclusivity would have expired by the time the initial judicial review was heard by the Federal Court in 2004. Prior to 2006, the duration of data exclusivity in Canada was five years, and Merck obtained market approval for Singulair® in 1998.²⁷⁷ Nevertheless, the protection of confidential information in the course of the market approval process for new drugs, as seen in the *Merck Frosst* decision, provides the contextual foundation for a discussion about data exclusivity.

In exploring the research question for this thesis, recall that the following three constructs must be addressed: 1) the regulation of clinical trials; 2) the data exclusivity right of pharmaceutical companies; and 3) the individual’s right to personal data protection. This thesis has completed the initial explanation of the first construct, the regulation of clinical trials. Confidential information was also discussed to illustrate the tension between access to information and the maintenance of its secrecy, in which this tension is evident in the pharmaceutical context. The discussion of confidential

²⁷⁵ *Merck Frosst* FC 2004, *supra* note 246 at para 15.

²⁷⁶ *Canada v Merck Frosst*, *supra* note 250 at para 28.

²⁷⁷ See *Merck Frosst* SCC, *supra* note 111 at para 11.

information has now laid the groundwork for the second construct, data exclusivity, which will be explored in the following section.

2.4. Data Exclusivity and Control over Confidential Information

Data exclusivity is related to the law of confidential information and thus relates to the free flow of information (or lack thereof). By affecting access to information about new drugs, data exclusivity also has an impact on public health. The present discussion will focus on the nature of data exclusivity and will discuss intellectual property in pharmaceutical research and development as well as the different perspectives regarding the impact of data exclusivity on public health outcomes and innovation.

2.4.1. Pharmaceutical Innovation and Intellectual Property Protection: Safeguarding Investment

A new drug that contains a medicinal ingredient that has not been previously approved by the Minister of Health is defined as an “innovative drug.”²⁷⁸ Accordingly, drug manufacturers that conduct clinical trials for innovative drugs are known as “innovative manufacturers” or “brand name drug manufacturers.” Once the Minister of Health approves the innovative drug and issues an NOC to the manufacturer, the drug becomes listed as a Canadian Reference Product.²⁷⁹

²⁷⁸ *Food and Drug Regulations*, *supra* note 5, s C.08.004.1(1):

innovative drug means a drug that contains a medicinal ingredient not previously approved in a drug by the Minister and that is not a variation of a previously approved medicinal ingredient such as a salt, ester, enantiomer, solvate or polymorph [emphasis in original].

²⁷⁹ *Ibid.*, s C.08.001.1 :

Canadian reference product means (a) a drug in respect of which a notice of compliance is issued under section C.08.004 or C.08.004.01 and which is marketed in Canada by the innovator of the drug; (b) a drug, acceptable to the Minister, that can be used for the purpose of demonstrating bioequivalence on the basis of pharmaceutical and, where

However, the road to approval of an innovative drug involves significant financial costs. A U.S. study from 2003 collected data from ten multinational pharmaceutical firms and estimated that the research and development cost per new drug was \$802 million, and that this cost increased to nearly \$900 million for research conducted after the drug was approved.²⁸⁰ These results were independently verified by another study from 2006 which used a publicly available data set.²⁸¹ Furthermore, the authors of the 2006 study estimated the costs per approved drug to be \$836 million before approval, and that the expected cost to large pharmaceutical firms for developing a drug ranged from \$521 million to \$2.1 billion.²⁸²

While no published estimate of the costs of developing a new drug can be considered a gold standard since clinical trials vary in their methods, data sources, samples,²⁸³ and the health conditions under investigation,²⁸⁴ it is nonetheless clear that pharmaceutical companies must invest vast amounts of capital into the research and development process, which can easily span a decade or more.²⁸⁵ The process also involves a high risk of failure, since it is estimated that fewer than 1% of compounds

applicable, bioavailability characteristics, where a drug in respect of which a notice of compliance has been issued under section C.08.004 or C.08.004.01 cannot be used for that purpose because it is no longer marketed in Canada; or (c) a drug, acceptable to the Minister, that can be used for the purpose of demonstrating bioequivalence on the basis of pharmaceutical and, where applicable, bioavailability characteristics, in comparison to a drug referred to in paragraph (a) [emphasis in original].

²⁸⁰ Joseph A DiMasi, Ronald W Hansen & Henry G Grabowski, “The Price of Innovation: New Estimates of Drug Development Costs” (2003) 22 *J Health Economics* 151 at 180.

²⁸¹ See Christopher P Adams & Van V Brantner, “Estimating the Costs of New Drug Development: Is it Really \$802 Million?” (2006) 25 *Health Affairs* 420 [Adams & Brantner].

²⁸² *Ibid* at 427.

²⁸³ Steve Morgan et al, “The Cost of Drug Development: A Systematic Review” (2011) 100 *Health Policy* 4 at 11.

²⁸⁴ See Adams & Brantner, *supra* note 281 at 427: The authors found considerable variation in the cost of developing different drugs, in which the estimated expected cost for developing a drug for HIV/AIDS was \$479 million, while the expected cost of developing a drug for rheumatoid arthritis was \$936 million.

²⁸⁵ Erika Lietzan, “The Myths of Data Exclusivity” (2016) 20 *Lewis & Clark L Rev* 91 at 107 [Lietzan, “Myths”].

examined during pre-clinical testing ultimately advance to the clinical trial stage,²⁸⁶ and drugs may also fail in late-stage clinical trials owing to their inability to outperform a placebo.²⁸⁷

Therefore, the expense and effort involved in pharmaceutical innovation ultimately gives rise to the perceived need for intellectual property protection. An innovative manufacturer will typically seek and obtain a patent for an innovative drug which will confer a monopoly of twenty years²⁸⁸ regarding the drug's manufacture, sale, and use.²⁸⁹ According to the *Patent Medicines (Notice of Compliance) Regulations*,²⁹⁰ the first person who files an NDS may submit a patent list to the Minister of Health for addition to the patent register.²⁹¹ Among other criteria, a patent list must identify the NDS to which the list relates; identify the medicinal ingredient, brand name, dosage form, strength, route of administration, and use set out in the NDS; and, for each patent on the list, contain a statement that the first person who filed the NDS to which the list relates is

²⁸⁶ Shammad Basheer, "The Invention of an Investment Incentive for Pharmaceutical Innovation" (2012) 15 *J World Intellectual Prop* 305 at 309.

²⁸⁷ *Ibid* at 310.

²⁸⁸ See *TRIPS*, *supra* note 52, art 33:

The term of protection available shall not end before the expiration of a period of twenty years counted from the filing date.

See also, *Patent Act*, *supra* note 74, s 44:

Subject to section 46, where an application for a patent is filed under this Act on or after October 1, 1989, the term limited for the duration of the patent is twenty years from the filing date.

²⁸⁹ *Patent Act*, *ibid*, s 42:

Every patent granted under this Act shall contain the title or name of the invention, with a reference to the specification, and shall, subject to this Act, grant to the patentee and the patentee's legal representatives for the term of the patent, from the granting of the patent, the exclusive right, privilege and liberty of making, constructing and using the invention and selling it to others to be used, subject to adjudication in respect thereof before any court of competent jurisdiction.

²⁹⁰ *Patent Medicines (Notice of Compliance) Regulations*, SOR/93-133.

²⁹¹ *Ibid*, s 4(1):

A first person who files or who has filed a new drug submission or a supplement to a new drug submission may submit to the Minister a patent list in relation to the submission or supplement for addition to the register.

the owner of the patent or has an exclusive license.²⁹² With respect to a patent on a patent list in relation to a NDS, the patent is eligible for addition to the patent register if it satisfies the criteria regarding the medicinal ingredient, formulation, dosage form, or use of the medicinal ingredient.²⁹³

The expiration of a patent on an innovative drug results in the loss of the manufacturer's monopoly over the drug's manufacture, sale, and use. Other drug manufacturers are subsequently free to engage in these activities regarding that drug. However, any new entrant to the Canadian market for the drug will also require an NOC from the Minister of Health. These later entrants are commonly known as "generic drug manufacturers," which simply means that these manufacturers are not innovators but produce drugs that are pharmaceutically equivalent and bioequivalent to the original innovative drugs. Instead of conducting their own clinical trials,²⁹⁴ a generic drug manufacturer can file an Abbreviated New Drug Submission (ANDS) to demonstrate that

²⁹² *Ibid*, s 4(4)(a)-(f).

²⁹³ *Ibid*, s 4(2):

A patent on a patent list in relation to a new drug submission is eligible to be added to the register if the patent contains

- (a) a claim for the medicinal ingredient and the medicinal ingredient has been approved through the issuance of a notice of compliance in respect of the submission;
- (b) a claim for the formulation that contains the medicinal ingredient and the formulation has been approved through the issuance of a notice of compliance in respect of the submission;
- (c) a claim for the dosage form and the dosage form has been approved through the issuance of a notice of compliance in respect of the submission; or
- (d) a claim for the use of the medicinal ingredient, and the use has been approved through the issuance of a notice of compliance in respect of the submission.

²⁹⁴ See *Food and Drug Regulations*, *supra* note 5, s C.08.002.1:

An abbreviated new drug submission or an abbreviated extraordinary use new drug submission shall contain sufficient information and material to enable the Minister to assess the safety and effectiveness of the new drug, including the following:

- (a) the information and material described in (i) **paragraphs C.08.002(2)(a) to (f), (j) to (l) and (o), in the case of an abbreviated new drug submission** [emphases added].

One thus observes that, unlike an NDS, an ADNS does not need to contain "detailed reports of tests made to establish the safety of the new drug for the purpose and under the conditions of use recommended" and "substantial evidence of the clinical effectiveness of the new drug for the purpose and under the conditions of use recommended" which are prescribed by paragraphs C.08.002(2)(g) and (h).

their drug is equivalent to a Canadian Reference Product in terms of pharmaceutical equivalence, bioequivalence, route of administration, and conditions of use.²⁹⁵ Section C.08.002.1 of the *Food and Drug Regulations* outlines the criteria for the content of an ANDS, which must consist of the identification of the Canadian Reference Product used in any comparative studies and evidence from comparative studies that demonstrates that the new drug is equivalent to the Canadian Reference Product.²⁹⁶

In this way, generic drug manufacturers do not have to incur the costs associated with conducting clinical trials. Competition in the marketplace also increases with the expiration of the patent on an innovative drug, which generally results in drug price reductions.²⁹⁷ Thus, generic drugs are also typically sold at cheaper prices than those charged by innovative drug companies. A report published by the Patented Medicine Prices Review Board found that, of a sample of 284 drugs, the price of a typical Canadian generic drug in 2013 was 39% of the corresponding price of the innovative drug, and in Ontario, the generic price was 31% of that for the innovative drug.²⁹⁸ The cheaper generic

²⁹⁵ *Ibid*, s C.08.002.1 (1):

A manufacturer of a new drug may file an abbreviated new drug submission or an abbreviated extraordinary use new drug submission for the new drug where, in comparison with a Canadian reference product,

- (a) the new drug is the pharmaceutical equivalent of the Canadian reference product;
- (b) the new drug is bioequivalent with the Canadian reference product, based on the pharmaceutical and, where the Minister considers it necessary, bioavailability characteristics;
- (c) the route of administration of the new drug is the same as that of the Canadian reference product; and
- (d) the conditions of use for the new drug fall within the conditions of use for the Canadian reference product.

²⁹⁶ *Ibid*, s C.08.002.1(a)-(e).

²⁹⁷ See Joel Lexchin, “The Effect of Generic Competition on the Price of Brand-Name Drugs” (2004) 68 *Health Policy* 47 at 48: For example, in Ontario in the 1990s, there was a 25% discount on the price of a drug where a single generic competitor was available, and this reduction in price increased to 50% or greater when there were four to five generic competitors.

²⁹⁸ Patented Medicine Prices Review Board, *Generic Drugs in Canada, 2013* (December 2014) at 7, available online: <http://www.pmprb-cepmb.gc.ca/CMFiles/NPDUIS/2013-GenReport/PMPRB_NPDUIS_GenericDrugs2013_2014-12_EN.pdf> (accessed April 15, 2017).

versions of drugs accordingly result in considerable cost savings to the consumer and ultimately promote access to affordable, essential medicines.

The enormous financial costs and labour associated with clinical trials and the ability to circumvent these efforts by generic manufacturers provide the initial context in which data exclusivity arises. As once observed by Binnie J., if innovation is the lifeblood of a modern economy, human ingenuity must be rewarded in order to further advance the frontiers of knowledge.²⁹⁹ Intellectual property protection thereby satisfies a person's entitlement to the "fruits of their labour" by allowing the innovator to exploit the subject matter of the protection for a defined period of time. Patent protection and data exclusivity arguably provide the means for exploitation. This perspective of data exclusivity's purpose, however, has created considerable controversy with respect to the impact on public health. This controversy largely has to do with arguments over the nature of data exclusivity and the extent of the protection it confers under the trade agreements, specifically TRIPS, from which it originates.

2.4.2. Nature of Data Exclusivity: Interpretative Context and International Trade

The term "data exclusivity" is not a legally defined term. It is nonetheless an apt description of the protection's effects on intellectual property rights holders. Recall that TRIPS and NAFTA both mandate the protection of confidential information.³⁰⁰ For example, under Article 39 of TRIPS, member states are required to protect "undisclosed information."³⁰¹ Article 39(3) contains the data exclusivity rules under TRIPS and

²⁹⁹ *Harvard College*, *supra* note 170 at para 4.

³⁰⁰ See *TRIPS*, *supra* note 52, art 39; *NAFTA*, *supra* note 51, art 1711.

³⁰¹ For example, Gervais notes that the word "information" in the expression "undisclosed information" under TRIPS "must be used in the widest sense, and covers all types of data, including formulas and test data, as long as the information is identifiable. Furthermore, the information being protected is not actually

mandates protection for “undisclosed” data, “the origination of which involves a considerable effort”³⁰² against “unfair commercial use” and “disclosure”:

Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.³⁰³

NAFTA contains similar language to Article 39(3) of TRIPS with respect to the obligation to protect test data against unfair commercial use and disclosure. Article 1711(5) states:

If a Party requires, as a condition for approving the marketing of pharmaceutical or agricultural chemical products that utilize new chemical entities, the submission of undisclosed test or other data necessary to determine whether the use of such products is safe and effective, the Party shall protect against disclosure of the data of persons making such submissions, where the origination of such data involves considerable effort, except where the disclosure is necessary to protect the public or unless steps are taken to ensure that the data is protected against unfair commercial use.³⁰⁴

Despite the aforementioned similarities between TRIPS and NAFTA, there is an important distinction between the two agreements regarding the duration of data exclusivity. Whereas TRIPS does not specify a minimum term of protection, Article 1711(6) of NAFTA mandates a “reasonable period” of protection of “not less than five years”:

Each Party shall provide that for data subject to paragraph 5 that are submitted to the Party after the date of entry into force of this Agreement, no person other than the person that submitted them may, without the latter's

undisclosed information, but rather, “information disclosed selectively and under precise conditions”: See Gervais, *supra* note 43 at 541.

³⁰² Based on the demands of the scientific process in developing a drug, it is clear that clinical trial data falls within the scope of “a considerable effort” in generating data. Gervais notes that “in many cases, (e.g. clinical trials), there will be no doubt as to the sufficiency of the efforts necessary to generate the data”: See Gervais, *ibid* at 545.

³⁰³ TRIPS, *supra* note 52, art 39(3).

³⁰⁴ NAFTA, *supra* note 51, art 1711(5).

permission, rely on such data in support of an application for product approval during a reasonable period of time after their submission. For this purpose, **a reasonable period shall normally mean not less than five years** from the date on which the Party granted approval to the person that produced the data for approval to market its product, taking account of the nature of the data and the person's efforts and expenditures in producing them. Subject to this provision, there shall be no limitation on any Party to implement abbreviated approval procedures for such products on the basis of bioequivalence and bioavailability studies [emphasis added].³⁰⁵

Data exclusivity therefore originates from TRIPS and NAFTA. These agreements mandate that, where drug manufacturers are required to submit test data to a regulatory agency in the course of a market approval process for new drugs, this data is confidential and must be protected as such. Members of the WTO, including Canada, that are signatories to TRIPS and NAFTA are accordingly required to implement data exclusivity obligations into their domestic legislation.³⁰⁶ Owing to the possibilities for economic sanctions for failure to comply with obligations under TRIPS and NAFTA, it is essential to determine the nature and scope of the rights that data exclusivity provides to the entities that generate confidential clinical trial information. The following two sections of this thesis will discuss the academic literature with respect to the purpose of data exclusivity.

³⁰⁵ *Ibid*, art 1711(6).

³⁰⁶ *Ibid*, art 105. See also *TRIPS*, *supra* note 52, art 1(1):

Members shall give effect to the provisions of this Agreement. Members may, but shall not be obliged to, implement in their law more extensive protection than is required by this Agreement, provided that such protection does not contravene the provisions of this Agreement. Members shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice.

2.4.3. Nature of Data Exclusivity: Perspective of Proponents – Protecting Public Health and Preventing Free-Riding

Proponents of data exclusivity typically characterize its purpose as a means to encourage drug research and development. For example, Erika Lietzan observes that, to ensure that “pioneers” do the necessary research for the benefit of subsequent applicants and patients alike, “some delay is necessary before that research may be used by others.”³⁰⁷ This delay will satisfy the needs of future generations of patients for as-yet undiscovered and undeveloped drugs by ensuring that innovative manufacturers do not face immediate competition from companies who circumvent research and pay “a fraction of the same price for market entry.”³⁰⁸ Public health concerns thus justify data exclusivity.³⁰⁹

In their analysis of the language used in Article 39(3) of TRIPS, G. Lee Skillington and Eric Solovy focus on the intentions of the TRIPS negotiators and also note that WTO panels and the WTO Appellate Body are “very reluctant to interpret provisions in a manner that leaves them without meaning and that makes them redundant.”³¹⁰ In addition, Skillington and Solovy assert that a “fundamental” purpose of data exclusivity protection is to provide incentives to bring new drugs to market, such that prohibiting reliance on an innovator’s data would be consistent with this purpose.³¹¹ Reliance on an innovative manufacturer’s data before the innovator has had the chance to recoup the costs of the efforts to generate the data would be unjust, since the competitor

³⁰⁷ Lietzan, “Myths,” *supra* note 285 at 122.

³⁰⁸ *Ibid* at 123.

³⁰⁹ The characterization of data exclusivity’s purpose as protecting public health has also been echoed by Canadian judges, which will be discussed in Chapter Three.

³¹⁰ G Lee Skillington & Eric M Solovy, “The Protection of Test and Other Data Required by Article 39.3 of the TRIPS Agreement” (2003) 24 Nw J Int’l L & Bus 1 at 33 [Skillington & Solovy].

³¹¹ *Ibid* at 33.

would not only receive a “free ride” on the innovator’s investment but would be in a better market position than the innovator, owing to the substantial economic savings from circumventing the clinical trial process.³¹² Skillington and Solovy thus conclude that the term “unfair” would also be interpreted in light of commercial consequences, and would be interpreted as prohibiting any reliance on an innovator’s data.³¹³ Logically, the TRIPS negotiators likely intended “unfair commercial use” of data to mean that the data will not be used to support or review submissions of second applicants, since to conclude otherwise would effectively give second applicants a commercial advantage because they did not have to generate their own data, unlike innovative manufacturers.³¹⁴

Daniel Gervais has similarly noted that uses of an innovator’s data by a competitor could be deemed unfair if they give the competitor a “springboard” to “shortcut” research and development efforts,³¹⁵ such that generic manufacturers who demonstrate bioequivalence to an innovative drug would be encompassed by this interpretation of the expression. Daria Kim has also observed that, according to WIPO’s *Model Provisions on Protection Against Unfair Competition*, disclosure of test or other data constitutes an act of unfair competition, since this disclosure may have similar detrimental effects on an enterprise in the same manner as unauthorized use of the information.³¹⁶

The prevention of “free-riding” upon an innovator’s work is also central to Lietzan’s argument that data exclusivity does not constitute a reward conferred on

³¹² *Ibid* at 30.

³¹³ *Ibid*.

³¹⁴ *Ibid* at 33.

³¹⁵ Gervais, *supra* note 43 at 545.

³¹⁶ Daria Kim, “Enabling Access to Clinical Trial Data: When is Unfair Use Fair?” (2015) 14 Chi-Kent J Intell Prop 521 at 526, citing World Intellectual Property Organization, *Model Provisions on Protection Against Unfair Competition* (1996) at para 6.26, available online: <[ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_832\(e\).pdf](ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_832(e).pdf)>.

innovative manufacturers by the government, which creates the perception that data exclusivity is “artificial and provided, as a benefit, to pioneers.”³¹⁷ Instead, Lietzan argues that data exclusivity is “not a grant of anything to anyone” but is “the absence of an abbreviated pathway,” since it does not prevent subsequent market entrants from “doing exactly what the first entrant did.”³¹⁸ Owing to reliance on an innovative manufacturer’s research, subsequent market entrants such as generic manufacturers face a reduced regulatory burden because approval of an innovative drug will eliminate “much of the trial and error” experienced by the innovative manufacturer.³¹⁹ Lietzan accordingly claims that reliance-based generic drug submissions should not be controversial with respect to proving use of the innovative manufacturer’s data, since a subsequent applicant “uses” an innovator’s research when it refers to the innovative drug by using the “fact” of the innovator’s approval to obtain its own approval.³²⁰

2.4.4. Nature of Data Exclusivity: Perspective of Opponents – Impeding Public Health while Providing “Double Protection”

Owing to the expense and effort involved in pharmaceutical innovation, incentives to innovate, through intellectual property protection, are arguably warranted. However, in the pharmaceutical context, the requirements to uphold intellectual property standards in TRIPS have inspired a continuous debate over effects on public health outcomes, since the higher costs of patented drugs erect financial barriers for access to

³¹⁷ Lietzan, “Myths”, *supra* note 285 at 104-105.

³¹⁸ *Ibid* at 110.

³¹⁹ *Ibid* at 105.

³²⁰ *Ibid* at 106.

essential medicines in developing countries.³²¹ At the WTO's Fourth Ministerial Conference in Doha, Qatar in November 2001, the WTO members affirmed that TRIPS "can and should be interpreted and implemented in a manner supportive of WTO members' right to protect public health, and in particular, to promote access to medicines for all."³²² In particular, owing to the inadequacy or outright lack of manufacturing capabilities in the pharmaceutical sector in developing countries, the members called for an "expeditious" solution to the difficulties faced by developing countries with respect to compulsory licensing under TRIPS.³²³ A compulsory license provides for flexibility in patent protection: it allows for "other use" of the subject matter of a patent without the authorization of the rights holder, thereby enabling a generic version of a patented medicine to be exported to developing countries that lack their own pharmaceutical manufacturing capacities.³²⁴ The 2003 decision of the WTO General Council thus addressed public health concerns of developing countries by waiving the domestic market

³²¹ See Michael Ravvin, "Incentivizing Access and Innovation for Essential Medicines: A Survey of the Problem and Proposed Solutions" (2008) 1 Pub Health Ethics 110.

³²² WTO, *Declaration on the TRIPS Agreement and Public Health*, WT/MIN(01)/DEC/2 (14 November 2001) at para 4, online: <https://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_trips_e.htm> (accessed June 27, 2017).

³²³ *Ibid* at para 6. See also Emily Ng & Jillian Clare Kohler, "Finding Flaws: The Limitations of Compulsory Licensing for Improving Access to Medicines – An International Comparison" (2008) 16 Health LJ 143 at 145: The authors note that Article 31(f) of TRIPS originally provided that compulsory licensing could only be used "predominantly" for the purposes of supply for the domestic market of the country in which the license was issued. This requirement accordingly created problems for the poorest countries that needed to import medicines because they did not possess the manufacturing capacity to produce their own generic drugs.

³²⁴ *TRIPS*, *supra* note 52, art 31. Article 31(f) also states that the phrase "other use" refers to use other than that allowed under Article 30 of TRIPS.

requirement under Article 31(f) of TRIPS,³²⁵ thereby enabling any country to receive imported medicines through compulsory licensing.³²⁶

Arguably, the above measures prevent patent holders from unduly emphasizing commercial interests at the expense of public health. However, it is important to note that Article 31 of TRIPS applies exclusively to the subject matter of *patent* protection and not that of data exclusivity. While Article 30 authorizes the provision of limited exceptions to the exclusive rights conferred by patent,³²⁷ there are no corresponding provisions under TRIPS or any WTO decisions that provide exceptions to data exclusivity protection. In this way, although data exclusivity functions in a manner akin to patent protection by providing a temporary monopoly on information generated in clinical trials and thus contributes to the delay of the market entry of cheaper drugs, there is a lack of formal mechanisms to address the potential impact of data exclusivity on public health outcomes.

Much of the opposition to data exclusivity occurs because of the uncertainty of interpretation of Article 39(3) of TRIPS regarding the rights conferred to confidential clinical trial data. For one thing, TRIPS does not mandate a uniform period of data exclusivity, unlike that seen for patent protection.³²⁸ Despite the fact that members are required to protect test data against “unfair commercial use,” TRIPS also does not

³²⁵ Use of the subject matter is generally restricted to domestic markets under *TRIPS, ibid*, art 31(f): “any such use shall be authorized predominantly for the supply of the domestic market of the Member authorizing such use.” Waiver of the domestic requirement under Article 31(f) was formally added to TRIPS as an amendment on January 23, 2017 in the form of Article 31*bis*.

³²⁶ See WTO, *Implementation of paragraph 6 of the Doha Declaration on the TRIPS Agreement and public health*, WT/L/540 and Corr 1 (1 September 2003), online: <
https://www.wto.org/english/tratop_e/trips_e/implem_para6_e.htm> (accessed June 27, 2017).

³²⁷ *TRIPS, supra* note 52, art 30:

Members may provide limited exceptions to the exclusive rights conferred by a patent, provided that such exceptions do not unreasonably conflict with a normal exploitation of the patent and do not unreasonably prejudice the legitimate interests of the patent owner, taking account of the legitimate interests of third parties.

³²⁸ See *TRIPS, ibid*, art 33, which mandates a twenty-year term of protection.

provide a clear definition of this expression.³²⁹ Antony Taubman thus proposes three possible forms of protection that can potentially arise in accordance with three corresponding interpretations of the Article 39(3) standard: 1) *proprietary rights in the form of data exclusivity*, in which protection against unfair commercial use would involve a fixed period of exclusive rights to data, such that any use of the data during this time would be deemed unfair; 2) a *compensatory regime*, in which the innovator cannot prevent others from using or referring to the data but is entitled to equitable financial compensation in order to remedy the “unfairness” of a competitor’s use of the data; and 3) *direct data protection*, in which there is no obligation to provide for exclusivity or compensation and where, although undisclosed data must be protected from unauthorized disclosure, “unfairness” is limited to data that is acquired by “dishonest means.”³³⁰ In any event, the arguably broad wording of Article 39(3) has led to controversy regarding its interpretation and, subsequently, the nature and extent of the protection conferred by the provision.

For example, owing to the fluidity in interpretation of “unfair commercial use,” some academics have concluded that the expression is not synonymous with exclusive proprietary rights. Peter Yu concludes that the scope of Article 39(3) is limited, in that it does not offer broad protection of test data but includes the following narrow conditions:

- 1) protection against unfair competition, which does not create exclusive rights in data;

³²⁹ One wonders why “unfair commercial use” is not defined under Article 39(3), since this “use” is particularly relevant to the scope of protection conferred by the provision. It is interesting to note that Article 39(2) of TRIPS, which protects information from being used “in a manner contrary to honest commercial practices,” specifically defines “a manner contrary to honest commercial practices” to mean “at least practices such as breach of contract, breach of confidence, and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition”: See *TRIPS, ibid.*, art 39(2), fn 10.

³³⁰ Antony Taubman, “Unfair competition and the financing of public-knowledge goods: the problem of test data protection” (2008) 3 *J Intell Prop L* 591 at 595.

and 2) protection for products that utilize new chemical entities, such that the provision should exclude entities that have been reformulated or sold for a new indication.³³¹

Similarly, in observing that Article 39(3) merely requires countries to protect data against “unfair commercial use,” Carlos Correa asserts that countries are not granted exclusive rights but instead have only the right to bring legal action against whoever has obtained commercial advantage through dishonest practices.³³² If the underlying rationale of data exclusivity is indeed to allow innovative manufacturers to recover their costs of research and development, this purpose protects investment rather than a creative or inventive outcome, which would be contrary to the very purpose of intellectual property rights.³³³ Unlike the TRIPS provisions related to trademark and patent, Correa observes that Article 39 of TRIPS does not use language that confers ownership rights, thereby supporting the notion that innovative manufacturers do not have exclusivity rights to trade secrets and test data.³³⁴ In addition, Correa asserts that the interpretation of “unfair commercial use” must be based on the ordinary meaning of the words therein.³³⁵ Correa observes that there is no universal rule to determine whether certain practices should be deemed unfair, since different countries will likely judge certain situations differently in accordance with their values and competitive advantage.³³⁶ Thus, Article 39(3) only applies when a competitor obtains a benefit or advantage as a result from unfair

³³¹ Peter K Yu, “The Political Economy of Data Protection” (2010) 84 Chi-Kent L Rev 777 at 783 [Yu].

³³² Carlos M Correa, “Bilateralism in Intellectual Property: Defeating the WTO System for Access to Medicines” (2004) 36 Case W Res J Int’l L 79 at 83.

³³³ *Ibid* at 83.

³³⁴ Carlos Maria Correa, “Unfair Competition under the TRIPS Agreement: Protection of Data Submitted for the Registration of Pharmaceuticals” (2002) 3 Chic Int’l L 69 at 82, referring to *TRIPS*, *supra* note 52, arts 16 (trademark) & 28 (patent). The provisions relating to patent expressly state that patent confers “exclusive rights” on its “owner.” The words “owner” and “exclusive right” are also found in Article 16 of TRIPS to describe the rights conferred for trademark.

³³⁵ *Ibid* at 77.

³³⁶ *Ibid*.

commercial practices, in which it is the qualification of the practice that is relevant rather than the mere existence of an advantage or benefit.³³⁷

In addition to interpretative issues surrounding Article 39(3) of TRIPS, another common concern among academics is the effects of the dual application of patent protection and data exclusivity. For example, Trudo Lemmens and Candice Telfer assert that data exclusivity confers a de facto extension of patent protection, which should already have been fair compensation for the investment in drug development.³³⁸ This patent-style protection on pharmaceutical products forces generic manufacturers to: a) either wait until the period of data exclusivity has passed; or b) invest in clinical test data without receiving the same financial reward that innovators receive from patent.³³⁹

Jerome Reichman similarly contends that longer terms of data exclusivity do not actually create greater incentives for conducting clinical trials, since they essentially allow innovative manufacturers to “have it both ways,” without accounting for the excess profits yielded, in many cases, by the overlapping patent and data exclusivity regimes.³⁴⁰

Yu thus asserts that, while the costs of clinical trials remain high and consist of a major portion of research and development costs for new drugs, innovative manufacturers have considerable incentives under the patent system, thereby rendering the need for data exclusivity laws to be “economically dubious.”³⁴¹

³³⁷ *Ibid* at 78.

³³⁸ Trudo Lemmens & Candice Telfer, “Access to Information and the Right to Health: The Human Rights Case for Clinical Trials Transparency” (2012) 38 *Am J L & Med* 63 at 85 [Lemmens & Telfer].

³³⁹ *Ibid* at 85.

³⁴⁰ Jerome H Reichman, “Rethinking the Role of Clinical Trial Data in International Intellectual Property Law: The Case for a Public Goods Approach” (2009) 13 *Marq Intell Prop L Rev* 1 at 41 [Reichman]. Addressing the question of “how much profit is too much” is beyond the scope of this thesis. Since a key purpose of a corporation is to make money for its shareholders, a comprehensive answer would need to reflect the realities of corporate ownership of intellectual property rights.

³⁴¹ Yu, *supra* note 331 at 784. Yu also notes that many innovative pharmaceutical companies receive “significant” support from public funding to conduct research and development.

There is merit in the concerns regarding the legitimacy of data exclusivity with respect to the “bargain” at the heart of intellectual property law. Data exclusivity laws confer exclusive rights in a manner akin to patent protection despite the differences between these regimes with respect to the public knowledge contributed by an innovator in exchange for a market monopoly. In Canada, for example, notwithstanding a confidentiality period of eighteen months that begins on the date of filing,³⁴² all patents, patent applications, and documents that are filed in connection with patents or applications are subject to public access and scrutiny.³⁴³ Patent is thus not a restraint on free competition. By contributing a new and useful technical achievement that others in the relevant field could not themselves have developed, disclosing the invention to the public in exchange for a legal monopoly actually helps to elevate the existing state of competition to the next highest level.³⁴⁴ In this way, public disclosure of an invention not only encourages people with the appropriate skills to innovate but also contributes to the education of the public at large. Owing to the requirement for direct public disclosure, it is therefore arguable that patent protection does promote creative outcomes in accordance with the purpose of intellectual property law.

However, it is more difficult to justify data exclusivity on the same grounds.

Since innovative drug manufacturers are not required to publicly disclose their clinical

³⁴² *Patent Act*, *supra* note 74, s 10(2)-(3):

...(2) Except with the approval of the applicant, an application for a patent, or a document filed in connection with the application, shall not be open to public inspection before a confidentiality period of eighteen months has expired;

(3) The confidentiality period begins on the filing date of the application or, where a request for priority has been made in respect of the application, it begins on the earliest filing date of any previously regularly filed application on which the request is based.

³⁴³ *Ibid.*, s 10(1):

Subject to subsections (2) to (6) and section 20, all patents, applications for patents and documents filed in connection with patents or applications for patents shall be open to public inspection at the Patent Office, under such conditions as may be prescribed.

³⁴⁴ Reichman, *supra* note 340 at 42.

trial data, the characterization of clinical trial data as a proprietary asset to which innovative manufacturers maintain exclusive rights seems to lack social utility that is readily apparent. Pamela Andanda also observes that data exclusivity may impede efforts by clinical researchers and regulatory authorities to share information that may potentially benefit clinical research participants, which constitutes a public health concern that has been “overshadowed” by the innovative industry’s preoccupation with preventing competition from generic manufacturers.³⁴⁵

In addition, the notion that generic manufacturers are free to conduct their own clinical trials may be illusory owing to both financial and ethical concerns. Generic manufacturers, by definition, do not have a patent which allows them to monopolize the market and so would not be able to charge consumers sufficient amounts of money to recoup the huge costs of clinical trials.³⁴⁶ Moreover, having a generic manufacturer repeat a pre-existing trial simply for the sake of conducting its own trial would ultimately deny some patients access to medicines³⁴⁷ and would submit research participants to unnecessary duplicate testing, which would be ethically problematic for patients who are asked to participate in placebo-controlled trials.³⁴⁸ Yu therefore declares that there are serious moral implications for introducing data exclusivity laws that would delay the entry of pharmaceuticals that would otherwise become readily available at the end of a patent term.³⁴⁹

³⁴⁵ Pamela Andanda, “Managing Intellectual Property Rights Over Clinical Trial Data to Promote Access and Benefit Sharing in Public Health” (2013) 44 Max Planck Institute for IP & Competition Law 140 at 142.

³⁴⁶ Reichman, *supra* note 340 at 5.

³⁴⁷ *Ibid* at 5.

³⁴⁸ Lemmens & Telfer, *supra* note 338 at 85.

³⁴⁹ Yu, *supra* note 331 at 785.

2.4.5. Nature of Data Exclusivity: Conclusion

Based on the above review of the literature on data exclusivity, one can conclude that the nature of data exclusivity remains unclear, in a manner similar to the uncertainty surrounding the nature of confidential information. What is clear, however, is that the characterization of data exclusivity depends on the perspective of the particular advocate, since persuasive arguments have been made by both proponents and opponents of the protection. Furthermore, as will be discussed in the next chapter, data exclusivity has been implemented in a way such that the generating entities of clinical trial data maintain exclusive rights of control for the term of protection.

Data exclusivity and patent protection function in similar ways through the grant of limited term monopolies. Some academics view data exclusivity as necessary to reward innovation and thus protect public health through the development of new medicines, while other commentators criticize data exclusivity as a detriment to public health by hindering access to medicines. Despite this debate over the purpose and impact of data exclusivity, however, this thesis established in the previous discussion of the nature of confidential information that the secrecy of confidential information has the potential to continue indefinitely. In contrast, since data exclusivity protection endures for a limited time, it can be considered as a *limitation* on secrecy for information that would otherwise remain forever secret. Classifying clinical trial data, such that it fits within the scope of data exclusivity protection and not that of trade secrets,³⁵⁰ leads to the situation where the initial restriction on access to information ultimately results in a

³⁵⁰ Please refer above to section 2.1.8 of this thesis with respect to the discussion establishing that clinical trial data does not constitute a trade secret.

greater benefit – access to otherwise permanently secret information – than would be obtained had the protection not existed in the first place.

2.5. Uniting the Constructs: Confidential Information, Data Exclusivity, and Personal Data Protection in the Context of Clinical Trials

The law of confidential information and data exclusivity protection concern the secrecy and maintenance of control over information, which often can be in direct opposition with public interest outcomes. By delaying the entry of cheaper drugs into the market, data exclusivity can contribute to financial barriers in accessing affordable medicines. Deschamps J., writing for the minority in the *Merck Frosst* case, observed that “access to information may be becoming the favourite battleground of innovative and generic drug manufacturers.”³⁵¹ The struggle between innovative and generic manufacturers over the issue of confidential information generated in clinical trials for new drugs constitutes one illustrative example of the different, yet compelling, interests of the multiple stakeholders that compete for control over the same information.

However, the discourse regarding data exclusivity is so focused on the struggle between the interests of innovative and generic manufacturers, access to medicines, and public health outcomes that it has neglected to consider the interest of another key stakeholder: that of the individual clinical trial participants with respect to their personal information. The failure to account for personal data protection is evident since no authors, whether or not they support or oppose data exclusivity protection, have addressed the reality that patient health information is collected in clinical trials and necessarily constitutes part of the *same set of test data*. Thus, it is also necessary to

³⁵¹ *Merck Frosst SCC*, *supra* note 111, per Deschamps J. at para 260.

clarify the individual patient's rights of control with respect to this data. The lack of guidance on this issue accordingly forms the basis of the research question of this thesis: whether the regimes of data exclusivity and personal data protection operate consistently with each other in terms of the rights that they protect.

2.5.1. Personal Data Protection and the Individual's Right to Control Information

Wilkinson, who has written extensively in the area of personal data protection,³⁵² argues that the role of personal data protection has been largely misunderstood by both the public and courts alike, owing to its overlapping vocabulary with privacy law.³⁵³ While privacy has been commonly understood as “the right to be let alone,”³⁵⁴ this classic understanding of privacy does not clarify the nature of privacy but makes a claim to legal or normative status.³⁵⁵ Instead, Wilkinson asserts that privacy may be better understood as a “*state of being let alone*” and further notes that there are important differences between privacy and personal data protection.³⁵⁶ Personal data protection is restricted to issues related to data, whereas privacy encompasses interests beyond informational privacy.³⁵⁷ Moreover, whereas personal data protection is confined by statute to

³⁵² For example, see: Perry & Wilkinson, *supra* note 99; and Wilkinson, “Confidential Information”, *supra* note 49.

³⁵³ Margaret Ann Wilkinson, “The Confidentiality of Seclusion: Studying Information Flows to Test Intellectual Property Paradigms,” in Courtney Doagoo et al (eds), *Intellectual Property for the 21st Century: Interdisciplinary Perspectives on Intellectual Property Law* (Toronto: Irwin Law, 2014), 72-94 at 80 [Wilkinson, “Confidentiality of Seclusion”].

³⁵⁴ Samuel D Warren & Louis D Brandeis, “The Right to Privacy” (1890) 4 Harvard L Rev 193 at 205.

³⁵⁵ Margaret Ann Wilkinson, “Battleground between New and Old Orders: Control Conflicts between Copyright and Personal Data Protection,” in Ysolde Gendreau, ed, *Emerging Intellectual Property Paradigm – Perspectives from Canada* [Queen Mary Studies in Intellectual Property series edited by Uma Suthersanen], (Cheltenham (UK): Edward Elgar, 2008), 227-266 at 245 [Wilkinson, “Control Conflicts”].

³⁵⁶ *Ibid* at 245.

³⁵⁷ *Ibid* at 246: Section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter], states that everyone has the right to be secure against unreasonable search or seizure. Wilkinson notes that section 8 has been interpreted to protect individuals against state incursion of privacy interests “beyond informational privacy.”

information about an identifiable individual,³⁵⁸ privacy encompasses rights to refuse to divulge *any* information held by an individual that the individual wishes to keep secret, including information about the individual.³⁵⁹

Wilkinson thus argues that personal data protection legislation is designed to regulate *organizations* that obtain information about individuals from various sources.³⁶⁰ Rather than regulating the flow of information between *individuals* in society,³⁶¹ personal data protection laws maintain a balance between individual privacy interests and the access of personal information by organizations once an individual “has had information about herself or himself come into the hands of an organization governed by [personal data protection] legislation.”³⁶² This interpretation of the goal of personal data protection is supported by the language used to articulate the purpose of Canada’s federal private sector personal data protection statute, PIPEDA:

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that **recognizes the right of privacy of individuals** with respect to their personal information **and the need of organizations** to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances [emphases added].³⁶³

The above provision of PIPEDA reflects the reality that personal information does not always remain exclusively in the hands of the individual. Furthermore, personal data protection acknowledges that there can be legitimate interests, other than that of the individual, involved with respect to access, use, and dissemination of this information.

³⁵⁸ See *PIPEDA*, *supra* note 101, s 2(1). The concept of identifiability and its relationship to personal information will be further addressed in Chapter Three.

³⁵⁹ Wilkinson, “Control Conflicts,” *supra* note 355 at 246.

³⁶⁰ Wilkinson, “Confidentiality of Seclusion,” *supra* note 353 at 81.

³⁶¹ *Ibid.*

³⁶² *Ibid.*

³⁶³ *PIPEDA*, *supra* note 101, s 3.

Both Wilkinson and Mark Perry have thus noted that, while personal data protection is closely related to privacy law, there is also a distinction between these two constructs with respect to the flow of information.³⁶⁴ Whereas privacy law focuses on reinforcing a person's desire for informational seclusion,³⁶⁵ personal data protection laws assume that the individual's personal information is not being held privately by the individual but has already made its way into the possession of an organization.³⁶⁶ Thus, personal data protection is concerned with the flow of information between individuals and organizations: instead of regulating *whether* information can be gathered from individuals or about individuals, personal data protection regulates *how* information is to be gathered about individuals.³⁶⁷

Since personal data protection statutes also restrict the scope of organizations' abilities to use and disseminate the collected information, Wilkinson argues that these statutes are an extension of the law of confidence, in which personal data protection laws mandate a relationship of confidence "between individuals providing information about themselves to organizations and the affected organizations."³⁶⁸ Indeed, the "essence" of the protection of confidential information, privacy, and personal data protection is to "exclude others completely from access."³⁶⁹ However, the individual's entitlement to confidentiality in information that is supplied to organizations is limited, under personal

³⁶⁴ Perry & Wilkinson, *supra* note 99 at 96.

³⁶⁵ For example, in *Jones v Tsige*, 2012 ONCA 32, 108 OR (3d) 241, the plaintiff and defendant did not know each other but worked at different branches of the same bank. Using her workplace computer, the defendant accessed and examined the plaintiff's private bank records on numerous occasions. The Ontario Court of Appeal thus recognized a tort of intrusion upon seclusion, which consists of 1) intentional conduct by the defendant; 2) invasion of the plaintiff's private affairs without lawful justification; and 3) that a reasonable person would regard the invasion as highly offensive causing distress, humiliation, or anguish.

³⁶⁶ Perry and Wilkinson, *supra* note 99 at 96.

³⁶⁷ Wilkinson, "Control Conflicts," *supra* note 355 at 244.

³⁶⁸ *Ibid* at 256.

³⁶⁹ Wilkinson, "Confidentiality of Seclusion", *supra* note 353 at 93.

data protection legislation, to confidences that involve information that is identified with that individual.³⁷⁰ Wilkinson observes that this narrow scope of legal protection for confidentiality likely constitutes the source of conceptual confusion between personal data protection and privacy.³⁷¹

James Moor has noted that there are situations in which people may not have *direct* control over the exchange of their personal information but there is no loss of privacy.³⁷² For example, personal information that is confided to a doctor may be shared with other medical professionals in the course of normal medical practice, and individuals also have little control over the way their personal information is stored on computer databases.³⁷³ Moor's observations are consistent with personal data protection laws, in that these laws do not promote the absolute secrecy of information but instead preserve an individual's right to confidentiality of personal information by providing controls over the ways in which organizations can collect, use, and disclose the individual's personal information. Furthermore, the ability of, say, the health care system to function effectively depends on the accuracy, completeness, and availability of health data: all participants in the health care system, including regulators and health care providers require high-quality information for informed decision-making.³⁷⁴ Personal data protection is accordingly concerned with both access *and* secrecy of personal information.

³⁷⁰ Wilkinson, "Control Conflicts", *supra* note 355 at 257.

³⁷¹ *Ibid* at 257.

³⁷² James Moor, "The Ethics of Privacy Protection" (1990) 39 Library Trends 69 at 75.

³⁷³ *Ibid*.

³⁷⁴ Lawrence O Gostin, "Health Information Privacy" (1995) 80 Cornell L Rev 451 at 451-452 [Gostin].

2.5.2. *The Right to Control One's Personal Information: The Importance of Consent*

The Supreme Court of Canada has recognized that an individual has an interest in the control of his or her personal information, which persists despite the fact that the information may be in the possession of another person or entity. The 1992 case *McInerney v. MacDonald* (“*McInerney*”)³⁷⁵ concerned a patient’s right of access to information in his or her medical records. The Supreme Court of Canada held that in the absence of regulatory legislation,³⁷⁶ patients are entitled, upon request, to inspect and copy all the information in their medical files which was considered in the administration of medical advice or treatment.³⁷⁷ According to LaForest J., the physician, institution, or clinic that compiles the medical records owns the physical records.³⁷⁸ However, LaForest J. also acknowledged that patients disclose sensitive information about the personal aspects of their lives when they approach a physician for health care. This information is “highly private and personal to the individual” and “goes to the personal integrity and autonomy of the patient.”³⁷⁹ Since information in a person’s medical records is essentially information about that person’s body, such information “remains in a fundamental sense one’s own, for the individual to communicate or retain as he or she

³⁷⁵ [1992] 2 SCR 138, 1992 CanLII 57 [*McInerney*]. The issues raised in this appeal were: 1) whether patient medical records prepared by a physician are the property of that physician or the patient; and 2) If patient medical records are indeed the property of the preparing physician, does a patient nonetheless have the right to examine and obtain copies of the documents in the record.

³⁷⁶ The dispute arose in the province of New Brunswick prior to the enactment of personal health information protection legislation. Rights of individual access rights to information in medical records are now enshrined under section 7 of New Brunswick’s *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05. Nonetheless, the case provides judicial guidance on the issue of an individual’s entitlement to control his or her personal health information.

³⁷⁷ *McInerney*, *supra* note 375 at para 39.

³⁷⁸ *Ibid* at para 14.

³⁷⁹ *Ibid* at para 18.

sees fit.”³⁸⁰ While an individual may decide to make personal information available to others to obtain benefits such as medical advice and treatment, the person has a “basic and continuing interest in what happens to this information, and in controlling access to it.”³⁸¹ LaForest J. observed:

The fiduciary duty to provide access to medical records is ultimately grounded in the nature of the patient's interest in his or her records...information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own. The doctor's position is one of trust and confidence. The information conveyed is held in a fashion somewhat akin to a trust. While the physician is the owner of the actual record, the information is to be used by the physician for the benefit of the patient. The confiding of the information to the physician gives rise to an expectation that the patient's interest in and control of the information will continue.³⁸²

LaForest J.'s statements emphasize the fundamental importance of the ability to control the information about oneself. This control is reflected in current personal data protection legislation in the health context.³⁸³ Personal health information protection statutes generally require individual consent for the collection, use, and disclosure of an individual's personal health information,³⁸⁴ and the individual is also entitled to access a record of his or her personal health information.³⁸⁵

³⁸⁰ *Ibid* at para 18, citing LaForest J. in *R v Dymnt*, [1988] 2 SCR 417, 1988 CanLII 10 at para 22. LaForest J.'s comments arose in the context of privacy in relation to information, which assumes that all information about an individual is fundamentally his or her own.

³⁸¹ *Ibid* at para 18.

³⁸² *Ibid* at para 22.

³⁸³ Chapter Three will explore the personal health information protection statutes in Canada.

³⁸⁴ For example, see Ontario's *Personal Health Information Protection Act*, RSO 2004, c 3 [*PHIPA*], s 29(1):

A health information custodian shall not collect, use or disclose personal health information about an individual unless,

- (a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
- (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act.

³⁸⁵ *Ibid*, s 52(1).

2.5.3. *Personal Information Protection: A Matter of Control and Not Ownership*

The concept of a fundamental interest in and right to control one's personal health information, as conceived by LaForest J. in *McInerney* and addressed in personal data protection statutes, raises the question of the definition of "control" itself. Solove observes that *control* over information is sometimes viewed as synonymous to *ownership* of the information, in which property in personal information is justified on the basis that personal information is an extension of one's personality or "selfhood."³⁸⁶ Advocates for the recognition of property rights in health data have asserted that private ownership would increase patients' power to block the unwanted use of their data and facilitate the wider availability of data for clinical and research uses.³⁸⁷

It is not clear what patient ownership of personal health information would entail in practice. Barbara Evans notes that, with respect to the issue of consensual access, use, and disclosure of personal data, the concept of property ownership in personal information fails to account for the reality that having a property right does not necessarily ensure its indefinite protection.³⁸⁸ Although personal data protection laws are intended to give individuals a right to control and access their personal information, they clearly do not confer an *absolute* right of control upon the individual with respect to his or her personal data. For example, an individual's right to access a personal health information record is subject to certain limitations, including situations where the record is subject to a legal privilege or where other legislation or a court order prohibits

³⁸⁶ Daniel J Solove, "Conceptualizing Privacy" (2002) 90 California L Rev 1087 at 1112 [Solove].

³⁸⁷ Barbara J Evans, "Much Ado about Data Ownership" (2011) 25 Harvard J L& Tech 69 at 77.

³⁸⁸ *Ibid* at 79. Evans notes that despite property ownership, an owner may be forced to relinquish his or her property in return for compensation that is externally set by a court, legislature, or administrative agency. It may even be the case that there is no compensation afforded to the owner, since the government has broad power to confiscate or interfere with property in the course of protecting public health, safety, and welfare.

disclosure to the individual.³⁸⁹ In addition, despite the general requirement for individual consent to disclosure of personal health information, there are some circumstances in which this information may be disclosed without the individual's consent, particularly when this disclosure would protect the public. For example, Ontario's *Personal Health Information Protection Act* ("PHIPA") authorizes the disclosure of personal health information where such disclosure is necessary to eliminate or minimize the risk of harm to "a person or group of persons."³⁹⁰ The limits on the extent to which one can control one's information under personal data protection legislation recognizes that there can be at least two, potentially competing interests with compelling claims to information.

In accordance with the traditional conception of privacy which emphasizes the ability to control information about oneself,³⁹¹ personal data protection ensures that organizations maintain the confidentiality of personal health information. On the other hand, exceptions to the confidentiality of personal health information acknowledge that an organization is sometimes justified to access, use, and disclose the information in fulfilment of another legitimate purpose. Regardless of whether one believes that personal information *should* be classified as property "owned" by the individual, the reality is that no personal data protection legislation has endorsed the notion that there is ownership in personal information. Instead, an individual has a "right" to control his or her personal information, which can be limited in certain circumstances. The question of

³⁸⁹ See *PHIPA*, *supra* note 384, s 52(a)-(f).

³⁹⁰ *Ibid*, s 40(1):

A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

³⁹¹ See Solove, *supra* note 386, and Charles Fried, "Privacy" (1968) 77 Yale LJ 475.

who *owns* the data is thus less important than the question of the rights and responsibilities of those who *hold* the data.³⁹²

The ability to control one's personal information is especially relevant in a digital world, where information can be shared instantaneously across multiple jurisdictions. Protecting the confidentiality of medical records is essential since health information "is perhaps the most intimate, personal, and sensitive of any information maintained about an individual."³⁹³ Lawrence Gostin, writing in 1995, observed that most individual health records were kept manually in "voluminous paper files"³⁹⁴ but asserted that "future health care information infrastructure will not merely contain automated records within each relevant institution" but would "electronically connect each of the vital components of the health care system, permitting the rapid exchange of health information."³⁹⁵

Patricia Goodman, writing in 2012, observed that Canadian jurisdictions were in the process of creating pan-provincial and territorial electronic health record networks, in respect of which the provinces and territories were at various stages of converting records containing personal health information into electronic form.³⁹⁶ Goodman found that individual consent to the collection of personal health information into electronic health

³⁹² Institute of Medicine, *Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk* (Washington, DC: The National Academies Press, 2015) at 42 [Institute of Medicine]. The authors also note that private sponsors of clinical trial data might claim ownership of the data, and that the language of research grants and contracts and the consent forms signed by clinical trial participants could delineate ownership of data. In light of these ownership claims and the fact that sponsors and other investigators are in possession of the data, it is important to ascertain the responsibilities of organizations with respect to the data.

³⁹³ Gostin, *supra* note 374 at 454.

³⁹⁴ *Ibid* at 457.

³⁹⁵ *Ibid* at 463. Gostin, at the time of writing, noted that health database organizations were already starting to collect, store, and use electronic data for the purposes of wide-scale population analyses.

³⁹⁶ Patricia Goodman, *Electronic Health Record Regulation in Canada: What the Patient Experience Reveals about the Pursuit of Legislative Harmonization*" (LLM Thesis, University of Western Ontario, 2012) at 3-4, online: <<http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=2055&context=etd>>.

records from non-electronic records was not required by any Canadian jurisdiction.³⁹⁷

Moreover, Michelle Gordon, writing in 2010, identified three potential privacy concerns associated with electronic health records – surveillance,³⁹⁸ aggregation,³⁹⁹ and secondary use⁴⁰⁰ – that, if not adequately addressed in legislation and policy, could cause individuals to lose control over their personal information in a digital environment.⁴⁰¹

Current technological realities with respect to the ways that personal health information is stored, handled, and processed by organizations thus support the notion that, instead of relying on ownership of personal health information to preserve an individual’s right to control this information, it is far more important to clarify the duties of organizations that have custody of personal health information with respect to the circumstances in which the information can be used and shared.

A clinical trial participant is wronged when there is improper disclosure of his or her data. For example, the inappropriate disclosure of patient health information can lead to negative social consequences, such as stigma or discrimination directed toward individuals who are identified as having mental illness or HIV infection or who engage in

³⁹⁷ *Ibid*, generally: Upon analyzing the legislative treatment of personal health information in electronic health records (EHRs) in each Canadian jurisdiction, Goodman grouped these jurisdictions into three models: 1) jurisdictions which had legislation specific only to the EHR environment; 2) jurisdictions that treated EHRs specifically within health-specific personal data protection legislation; and 3) jurisdictions that did not have health-specific personal data protection or EHR provisions, such that general personal data protection legislation applied. Within these models, Goodman found that individual consent to collection for personal health information in EHRs was not required by any of the jurisdictions.

³⁹⁸ Michelle Erin Gordon, *A Framework for the Protection of Privacy in an Electronic Health Environment* (LLM, University of Toronto, 2010) at 69, online: <

https://tspace.library.utoronto.ca/bitstream/1807/24573/1/Gordon_Michelle_E_201006_LLM_Thesis.pdf>:

Gordon states that individuals may be concerned that their personal health information is being inappropriately collected by the “wrong” individuals, such as researchers or the government, or that personal health information is being improperly collected, “either in excess or for incongruous purposes.”

³⁹⁹ *Ibid* at 72: Gordon defines aggregation as “the gathering of pieces of information about a person which, when combined, can create a greater picture about that person that he or she would not have anticipated when the original, individual pieces of information were collected.”

⁴⁰⁰ *Ibid* at 73: Gordon defines secondary use as “the use of information for purposes unrelated to the purposes for which the information was initially collected without the consent of the individual to whom the information pertains.”

⁴⁰¹ *Ibid* at 69.

activities such as sex work or substance abuse.⁴⁰² Moreover, with respect to the risks and benefits of disclosing information, some researchers observe that decisions by policy makers and committees do not usually consider subjective personal distinctions but instead instigate sweeping actions that apply to everyone in the same manner.⁴⁰³ While sharing information about sexual abuse, abortion, or depression medication may be liberating for one person, it may be harmful to another.⁴⁰⁴ It is important to expressly define the criteria for identifiability, since data such as the sex, age, and geographic location of research participants can reveal participants' identities if they are triangulated with other databases.⁴⁰⁵ Eloise Gratton has accordingly noted that it is not always clear at what point a particular piece of data can be said to "identify" an individual.⁴⁰⁶

2.6. Conclusion

Ultimately, the goal of this chapter was to illustrate the tension between access and secrecy of information. To achieve this purpose, this chapter explored the law of confidential information and the protection afforded to different types of confidential information. The theoretical background regarding the nature of the various concepts discussed in this chapter (confidential information, the regulation of medicines, data exclusivity, and personal data protection) demonstrates the reality that multiple stakeholders can have different but persuasive claims to access and control the same set

⁴⁰² Institute of Medicine, *supra* note 392 at 51.

⁴⁰³ Latanya Sweeney, Akua Abu & Julia Winn, *Identifying Participants in the Personal Genome Project by Name*, Data Privacy Lab: Harvard University (April 24, 2013), online: <<https://dataprivacylab.org/projects/pgp/1021-1.pdf>> (accessed June 20, 2017) at 1 [Sweeney et al].

⁴⁰⁴ *Ibid* at 1.

⁴⁰⁵ Michelle M Mello et al, "Preparing for Responsible Sharing of Clinical Trial Data" (2013) 369 N Eng J Med 1651 at 1653.

⁴⁰⁶ Eloise Gratton, "If Personal Information is Privacy's Gatekeeper, Then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information" (2014) 24 Alb LJ Sci & Tech 105 at 124 [Gratton].

of information. With respect to confidential information, these claims are best understood in terms of *rights of control* rather than ownership. Indeed, the law of confidential information in Canada is such that the protection of confidential information is based on the duty of confidence. Data exclusivity provisions in trade agreements do not mention ownership of data, and Canadian personal data protection legislation, such as PIPEDA, does not protect personal information based on ownership but instead recognizes the “right of privacy of individuals.”⁴⁰⁷

However, despite the essential role of individual clinical trial participants in pharmaceutical innovation, the importance of personal data protection and the rights of the individual to control personal information have been completely forgotten in the theoretical discourse on data exclusivity. This situation accordingly raises questions about whether the individual’s right to control personal data, though subject to certain limitations, is also abrogated by the operation of data exclusivity laws. Chapter Three will focus on the implementation of data exclusivity and personal data protection in Canada. In particular, the chapter will consist of an analysis of the legislative provisions of data exclusivity followed by their interpretation in recent Canadian case law. Subsequently, the chapter will offer an analysis and discussion of Canadian public and private sector personal data protection legislation and health-specific personal data protection statutes in order to determine whether the legislative regimes of data exclusivity and personal data protection operate consistently with each other in Canadian law.

⁴⁰⁷ See *PIPEDA*, *supra* note 101, s 3.

Chapter 3 – Data Exclusivity and Personal Data Protection in Canada

3.1. Data Exclusivity in Canadian Legislation

Just as “data exclusivity” is not legally defined in international instruments, it is also not a defined term in Canadian law. As this chapter will demonstrate, the term “data exclusivity” has largely been used in relation to the practical effects of the protection on the flow of the information generated in clinical trials.

Canada’s data exclusivity laws arise from the authority granted by Parliament to the Governor in Council under the *Food and Drugs Act*, in which section 30(3) confers power upon the Governor in Council to enact regulations that expressly implement Canada’s data exclusivity obligations under TRIPS and NAFTA:

Without limiting the power conferred by any other subsection of this section, **the Governor in Council may make any regulations** that the Governor in Council considers necessary **for the purpose of implementing**, in relation to drugs, **Article 1711 of the North American Free Trade Agreement and paragraph 3 of Article 39 of the Agreement on Trade-related Aspects of Intellectual Property Rights** set out in Annex 1C to the WTO Agreement [emphases added].⁴⁰⁸

Thus, it is clear that data exclusivity is *not* a Canadian conception but was instead forced upon Canada in the course of trade negotiations. The *Food and Drugs Act* is the enabling statute of the *Food and Drug Regulations*, which contain Canada’s data exclusivity provisions. There have been two different versions of this framework since Canada’s data exclusivity obligations first arose under TRIPS and NAFTA in the 1990s. The following section will describe the former version of these provisions and how judicial interpretation of the language therein ultimately led to amendments which resulted in Canada’s current regulatory scheme.

⁴⁰⁸ *Food and Drugs Act*, *supra* note 208, s 30(3).

3.1.1. Implementing Data Exclusivity into Canadian Legislation: Judicial Interpretation of the First Regulation

Canada introduced its first data exclusivity framework in 1995.⁴⁰⁹ Under this framework, section C.08.004.1 of the *Food and Drug Regulations* mandated a minimum period of five years with respect to reliance on an innovative manufacturer's data:

Where a manufacturer files a new drug submission, an abbreviated new drug submission, a supplement to a new drug submission or a supplement to an abbreviated new drug submission for the purpose of establishing the safety and effectiveness of the new drug for which the submission or supplement is filed, and the Minister examines any information or material filed with the Minister, in a new drug submission, by the innovator of a drug that contains a chemical or biological substance not previously approved for sale in Canada as a drug, **and the Minister, in support of the manufacturer's submission or supplement, relies on data contained in the information or material filed by the innovator, the Minister shall not issue a notice of compliance in respect of that submission or supplement earlier than five years after the date of issuance to the innovator of the notice of compliance or approval to market that drug**, as the case may be, issued on the basis of the information or material filed by the innovator for that drug [emphases added].⁴¹⁰

At first glance, this first version of section C.08.004.1 appears to be consistent with Canada's obligations under TRIPS and NAFTA, particularly with respect to the specified minimum period of protection mandated by Article 1711(6) of NAFTA. However, judicial interpretation of this provision considerably weakened data exclusivity protection for innovative manufacturers.

For example, the applicability of section C.08.004.1 concerning the Minister's reliance upon an innovative manufacturer's data was debated in *Bayer Inc. v. Minister of Health*.⁴¹¹ Specifically, the issue was whether the Minister would need to rely on data contained in an innovative manufacturer's NDS to establish the safety and efficacy of a

⁴⁰⁹ See *Bayer Inc v Canada (Attorney General)*, [1999] 1 FC 553, 83 ACWS (3d) 1028 at para 8 [Bayer FC].

⁴¹⁰ *Food and Drug Regulations*, CRC 1978, c 870, s C.08.004.1(1).

⁴¹¹ *Bayer FC*, *supra* note 409.

second manufacturer's drug, thereby triggering the application of section C.08.004.1 and thus imposing a delay of five years upon the second manufacturer. Bayer Inc. ("Bayer") argued that, if a second manufacturer filed an ANDS naming Bayer's drug as the Canadian Reference Product, the Minister would, inevitably, nearly always rely on the data contained in Bayer's NDS because an NOC would only have been issued to Bayer based on the safety and efficacy information in the NDS. Conversely, counsel for the Minister of Health argued that the Minister relies on the information contained in the ANDS itself without referring to materials previously filed by the innovative manufacturer.

Evans J. ultimately agreed with the Minister of Health. With respect to the scope of section C.08.004.1, he concluded:

"...this provision was not intended to create a protection analogous to a patent for the benefit of nearly all the innovators of new drugs who have obtained a NOC. I do not accept the submission that the Minister "relies" on the innovator's information for the purposes of C.08.004.1 when considering an ANDS or a NOC, where the Minister issues the NOC solely on the basis of the information contained in the ANDS...**the word adverb "indirectly" should not be read into C.08.004.1(1) so as to broaden the scope of the verb "relies"** [emphasis added].⁴¹²

The Federal Court of Appeal subsequently upheld the decision of Evans J. and also rejected the notion that the Minister could not issue an NOC to a second manufacturer earlier than five years after the issuance of an NOC to an innovative manufacturer.⁴¹³ The Court observed that the minimum five year protection under section C.08.004.1(1) would not apply if the second manufacturer could demonstrate in an ANDS that its drug was the pharmaceutical and bioequivalent of the innovator manufacturer's drug. The protection would thus apply only if the Minister "examines and relies upon information filed by the

⁴¹² *Ibid* at para 37.

⁴¹³ (1999) 243 NR 170, 89 ACWS (3d) 354 [*Bayer* FCA].

innovator in its NDS,” since the safety and efficacy of the drug would only be established by reference to confidential information provided by the innovative manufacturer.⁴¹⁴ The Court accordingly rejected Bayer’s argument that the Minister implicitly examined and relied on confidential information in a NDS whenever an ANDS is filed by a second manufacturer. Instead, the Court concluded that the regulation merely contemplated that the Minister “may or may not examine and rely upon confidential information filed by the innovator,” since to read the provision otherwise would effectively grant a minimum five-year market protection to an innovative manufacturer when an ANDS was filed by a second manufacturer.⁴¹⁵

The *Bayer* decision thus authorized the issuance of an NOC to a generic drug manufacturer as soon as the manufacturer was able to establish, on the basis of an ANDS, that its product was equivalent to an innovative manufacturer’s drug. Since this narrow interpretation of the data exclusivity regulation would essentially result in the non-application of the minimum five-year term of protection to an innovative manufacturer’s data in many, if not most, cases,⁴¹⁶ the *Bayer* case significantly weakened data exclusivity protection in Canada and, arguably, favoured generic manufacturers at the expense of innovative manufacturers.

Perhaps unsurprisingly, the *Bayer* decision led to tension between the U.S. and Canada with respect to Canada’s data exclusivity obligations. In 2003, the U.S. included

⁴¹⁴ *Ibid* at para 8:

It is only this use of that confidential information by the Minister on behalf of the generic manufacturer that gives rise to the minimum five year protection from competition for the innovator.

⁴¹⁵ *Ibid* at para 9.

⁴¹⁶ One legal commentator has noted that actual examination of information by the Minister rarely occurs, such that data exclusivity protection would not be effective where bioequivalence formed the basis of a submission by a generic manufacturer: See Brian W Gray, *Proposed Changes to Canadian Drug “Linkage” PM(NOC) Regs and Data Exclusivity Provisions*, McCarthy Tétrault (July 28, 2006), online: <http://www.mccarthy.ca/article_detail.aspx?id=2766>(accessed April 14, 2017).

Canada on the Watch List in its Special 301 Report.⁴¹⁷ The report claimed that Canada “does not provide effective data exclusivity protections, and systematic inadequacies in Canadian administrative and judicial procedures allow entry of infringing generic versions of patented medicines into the marketplace.”⁴¹⁸ This view of Canadian data exclusivity law was also consistent with that of some legal commentators, who called the judicial reasoning in *Bayer* “flawed in several ways”: aside from the fact that the meaning of the word “rely” in the English language does not mean “review” or “examine,” the right to exclusive use of data is consistent with one of the key purposes of the data exclusivity regulation, which is to encourage the testing and entry of new drugs into the marketplace.⁴¹⁹

In response to these criticisms, Canada’s federal government announced proposed amendments to the data exclusivity framework in December 2004, and acknowledged that Canada had not implemented its data exclusivity obligations in a manner that “automatically” prohibited reliance on an innovative manufacturer’s data for a minimum period of time.⁴²⁰ The new data exclusivity regulation, which came into force on October 5, 2006,⁴²¹ constitutes the current state of data exclusivity protection in Canada.

⁴¹⁷ The Special 301 Report is prepared by the Office of the United States Trade Representative and constitutes an annual review of the global state of intellectual property rights protection and enforcement. See: Office of the United States Trade Representative, online: <<https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications>> (accessed April 14, 2017).

⁴¹⁸ Office of the United States Trade Representative, *2003 Special 301 Report*, (May 1, 2003) online: <https://ustr.gov/archive/assets/Document_Library/Reports_Publications/2003/2003_Special_301_Report/as_set_upload_file665_6124.pdf> at 19 (accessed April 14, 2017).

⁴¹⁹ Skillington & Solovy, *supra* note 310 at 41.

⁴²⁰ Government of Canada, *News Release: Government of Canada Proposes Amendments to Intellectual Property Rules for Pharmaceuticals*, (Ottawa: December 13, 2004) online: <<https://www.canada.ca/en/news/archive/2004/12/government-canada-proposes-amendments-intellectual-property-rules-pharmaceuticals.html?=&wbdisable=true>> (accessed April 15, 2017).

⁴²¹ *Regulations Amending the Food and Drug Regulations (Data Protection)*, SOR/2006-241.

3.1.2. Strengthening Data Exclusivity in Canada: The Data Protection Regulation

The amended section C.08.004.1 of the *Food and Drug Regulations*, now known as the “Data Protection Regulation” (“DPR”), has expanded the scope of data exclusivity protection. For instance, section C.08.004.1(3) reads:

If a **manufacturer** seeks a notice of compliance for a new drug on the basis of a **direct or indirect comparison** between the new drug and an innovative drug,

(a) the **manufacturer may not file** a new drug submission, a supplement to a new drug submission, an abbreviated new drug submission or a supplement to an abbreviated new drug submission in respect of the new drug before the end of a period of **six years** after the day on which the first notice of compliance was issued to the innovator in respect of the innovative drug; and

(b) the **Minister shall not approve that submission or supplement and shall not issue a notice of compliance** in respect of the new drug before the end of a period of **eight years** after the day on which the first notice of compliance was issued to the innovator in respect of the innovative drug [emphases added].⁴²²

The amendments strengthen data exclusivity in a number of ways. First, under section C.08.004.1(3), it is now the *manufacturer’s* reliance that is relevant rather than that of the Minister. This provision essentially incorporates the appellant’s position in *Bayer* with respect to reliance of a generic manufacturer on an innovative manufacturer’s NDS materials, in that an ANDS “will merely purport to establish that [the generic manufacturer’s] drug is the pharmaceutical equivalent and bioequivalent” of the innovative drug, and “will not contain any independent evidence of the safety and effectiveness” of the generic product.⁴²³ Furthermore, section C.08.004.1(3) expressly includes the notion of “indirect” reliance on an innovative manufacturer’s data, thereby clarifying interpretive difficulties regarding actual or “implied” reliance. Perhaps most striking, the amended section now confers a total protection period of eight years, compared to the five years under the previous regulation, with mandatory delays on the

⁴²² *Food and Drug Regulations*, *supra* note 5, s C.08.004.1(3).

⁴²³ *Bayer FC*, *supra* note 409 at para 29.

filing of submissions and issuance of an NOC. For a six-year period, a generic manufacturer cannot file *any* submission to seek regulatory approval, and the provision also prohibits the Minister of Health from issuing an NOC to a generic manufacturer for an additional two years after the six-year period elapses.

As mentioned in Chapter Two, there are differences between TRIPS and NAFTA with respect to the mandated length of data exclusivity protection. While NAFTA requires member states to grant a five-year minimum term of protection, TRIPS does not mandate a minimum term of data exclusivity protection and instead leaves member states free to address the issue according to their own preferences. However, there is nonetheless an important similarity between both agreements regarding the permitted scope of intellectual property protection, since both TRIPS and NAFTA authorize their member states to enact more extensive protection than that required therein.⁴²⁴ Where there is a mandatory minimum period of protection and if the phrase “more extensive” protection also encompasses the length of protection, member states are within their legal rights to select and implement a term that exceeds the minimum requirement into their domestic legislation. However, if the purpose of a regulatory regime in the pharmaceutical context is to protect public health, the state government has a duty to consider the potential impact of any proposed legislation on the citizens of the state. Such policy issues are also an essential factor in the determination of the appropriate length of data exclusivity protection in Canadian legislation.

⁴²⁴ See *TRIPS*, *supra* note 52, art 1:

...Members may, but shall not be obliged to, implement in their law more extensive protection than is required by this Agreement, provided that such protection does not contravene the provisions of this Agreement.

See also, *NAFTA*, *supra* note 51, art 1702:

A Party may implement in its domestic law more extensive protection of intellectual property rights than is required under this Agreement, provided that such protection is not inconsistent with this Agreement.

Before passage of the new data exclusivity regime, Health Canada accepted submissions from various interested parties to ascertain the regulatory impact of the proposed amendments to the DPR. Health Canada received representations from 43 stakeholders, including innovative and generic manufacturers and their trade associations, members of parliament, law firms, provincial and territorial Ministers of Health, and consumer groups.⁴²⁵ These submissions reflected a clear difference in perspectives between the innovative and generic pharmaceutical industries with respect to the appropriate duration of data exclusivity protection. The generic drug industry objected to the proposed eight-year term, observing that this term would impose a delay on generic approval for a period that was three years longer than that mandated by NAFTA and in other jurisdictions such as the U.S.⁴²⁶ In contrast, the innovative drug industry supported the eight-year term of protection but encouraged the government to adopt a period of protection consistent with that of the European Union,⁴²⁷ which had, since November 30, 2005, begun to offer a ten-year term of protection with the possibility of an extension to eleven years for new therapeutic indications.⁴²⁸ Therefore, although Pei-Kan Yang suggests that Canada may have “overreacted” in its attempt to improve compliance with TRIPS and NAFTA,⁴²⁹ Canada’s eight-year term of protection actually constitutes a midpoint between five years and eleven years, thus reflecting an apparent effort to strike a balance between the two divergent terms of protection recommended by the innovative and generic drug industries.

⁴²⁵ Canada Gazette, *Regulatory Impact Analysis Statement*, Part II, (2006) 140(21), 1495 at 1500.

⁴²⁶ *Ibid* at 1501: the U.S. currently offers a five-year term of protection.

⁴²⁷ *Ibid* at 1499.

⁴²⁸ *Ibid* at 1501.

⁴²⁹ Pei-Kan Yang, “Current Developments of Canada’s Data Exclusivity Regime: How Does Canada React to NAFTA, TRIPS, and Dangle between Pharmaceutical Innovation and Public Health?” (2009) 4 Asian J WTO & Int’l Health L & Pol’y 65 at 68.

3.1.3. *Judicial Interpretation of the Data Protection Regulation in Canadian Case Law*

In *Canadian Generic Pharmaceutical Assn. v. Canada (Minister of Health)*,⁴³⁰

Canada's new 2006 DPR was challenged on the basis that the protection was *ultra vires* the federal legislative authority. Mandamin J. of the Federal Court addressed the following substantive issues: a) whether the DPR was *intra vires* the federal legislative powers pursuant to subsection 91(27) of the *Constitution Act, 1867*; b) whether the DPR and subsection 30(3) of the *Food and Drugs Act* were *intra vires* the federal legislative powers (as matters of national concern or the general regulation of trade and commerce); and c) whether the DPR was invalid owing to lack of rational connection to authority granted under section 30(3) of the *Food and Drugs Act* or because section 30(3) was an impermissible sub-delegation by Parliament.⁴³¹

Notably, this case illustrates the tension between the innovative and generic drug industries with respect to the nature and scope of data exclusivity protection. The first applicant, the Canadian Generic Pharmaceutical Association (CGPA),⁴³² emphasized the importance of low-cost generic drugs.⁴³³ The ability of generic manufacturers to receive market approval for their drugs plays an essential role in controlling drug prices in Canada, since upon market entry, the price of a generic drug is typically 30-50% below that of an innovative drug. The CGPA accordingly estimates that the monopoly imposed by the DPR cost the healthcare system \$500 million in lost savings. Secondly, the CGPA asserted that, where the generic manufacturer submits an ANDS, the Minister does not actually rely on an innovative manufacturer's clinical and pre-clinical studies in assessing

⁴³⁰ 2009 FC 725, 348 FTR 29 (Eng) at paras 78-79 [*Canadian Generic FC*].

⁴³¹ *Ibid* at para 42. "*Ultra vires*" means "in excess of powers." For example, a provision is *ultra vires* if it constitutes an invalid exercise of the power or authority granted to an entity by law. Conversely, "*intra vires*" means "within the powers."

⁴³² The CGPA consists of an association of generic drug manufacturers and suppliers.

⁴³³ *Canadian Generic FC*, *supra* note 430 at para 44.

the safety and efficacy of a generic drug.⁴³⁴ Instead, both the generic manufacturer and the Minister rely on: a) the fact that an NOC has previously been issued for a Canadian Reference Product; b) the fact that the Canadian Reference Product is being marketed in Canada; and c) the information and material in the ANDS. With respect to the validity of the DPR, Mandamin J. noted the CGPA's claims that the DPR was beyond the scope of subsection 30(3):

Permitted regulations must not restrict the authority conferred elsewhere in the Act, they must only apply to trade secrets or undisclosed data, and must affect only the person who "relies on" such data, and only for a "reasonable period", normally five years. The *Data Protection Regulation* exceeds these limitations; it creates a new intellectual property regime without statutory authority.⁴³⁵

On the other hand, Canada argued that the DPR was *intra vires* the federal legislative powers under section 91(27) of the *Constitution Act, 1867*. In particular, Canada asserted that the protection of public health and safety is a valid exercise of the federal government's criminal law power, and that the DPR contributes to the protection of public health and safety. By prohibiting all drugs except those that have been proven to be safe and effective, the DPR constitutes an integral part of the overall scheme concerning the marketing of drugs in Canada. In its submission, Canada emphasized the public safety elements of the *Food and Drug Regulations*, including the goal of "minimizing the potential for marketing unsafe drugs while maximizing the potential for

⁴³⁴ *Ibid* at para 44.

⁴³⁵ *Ibid* at para 115. Here, the CGPA appears to assert that the protection should endure only for five years. While NAFTA certainly provides a "reasonable period" of five years, one must note that TRIPS does not mandate a specific term of protection, and the DPR pertains to both NAFTA and TRIPS. Most important, as mentioned previously, member states under both of these agreements are within their legal rights to enact more extensive protections. In addition, the CGPA claims that the DPR creates a "new intellectual property regime without statutory authority." However, the DPR is arguably consistent with TRIPS, which mandates the freedom of member states to determine the appropriate method of implementing data exclusivity obligations into their own legal systems and practice: see *TRIPS*, *supra* note 52, art 1.

safe drugs to be readily accessible in the market”⁴³⁶ and the requirement for exhaustive, complete, and accurate information on the safety and effectiveness of a new drug.”⁴³⁷

Moreover, Canada acknowledged the issue of balance between the interests of generic and innovative manufacturers. In providing for an abbreviated process to prove the safety and efficacy of a new drug, the regulatory scheme also provides for competition in the marketplace by lowering the cost of drugs for the public and reducing the testing required for human subjects. Nevertheless, the abbreviated process must be subject to constraints (through data exclusivity) in order to avoid reducing the number of submissions for approval for innovative drugs. While these constraints may appear to relate to unfair commercial practices that would fall within the scope of provincial legislative powers, they are an essential component of the overall scheme of criminal law and are implemented to protect public safety.

In the end, contrary to the perspective of the CGPA, Mandamin J. observed that making a generic version of an approved drug circumvents the need to generate the requisite research and clinical data. Proof of safety and efficacy of a generic drug by comparing it to a Canadian Reference Product thus “necessarily relies on the earlier NDS information” submitted by an innovative manufacturer.⁴³⁸ In reaching this conclusion, Mandamin J. noted the perspective of Binnie J. of the Supreme Court of Canada with respect to reliance on an innovator’s submission:

Generally speaking, the “second person” intends to manufacture and distribute a “copy-cat” version of the active medicinal ingredient. If it copies the approved product, it can rely on the safety and efficacy data and the clinical studies

⁴³⁶ This balance thus reflects the theory that, since every new drug has the potential to be harmful even after it has been approved, there is a degree of risk accepted by the social collective whenever the government approves a new drug. See Chapter Two of this thesis: Erika Lietzan, “Transparency Initiatives”, *supra* note 222 at 78.

⁴³⁷ *Canadian Generic FC*, *supra* note 430 at para 48.

⁴³⁸ *Ibid* at para 130.

submitted by the “innovator” first person. Such reliance reduces the amount of required supporting data and the approval time, and the shortened submission is therefore known as an Abbreviated NDS (ANDS).⁴³⁹

Mandamin J.’s conclusion with respect to reliance makes logical sense. Although the Minister may review the ANDS material without having to refer to the original NDS submission, the reality is such that the evidence in the ANDS would not exist but for the Canadian Reference Product with which to compare the generic drug. This interpretation is accordingly consistent with the perspective of Lietzan, mentioned in Chapter Two, who asserted that there should be no question of reliance where an abbreviated submission uses the “fact” of the innovator’s approval as a comparison.⁴⁴⁰

As mentioned earlier in Chapter Two, the protection of confidential information appears to lack a public interest⁴⁴¹ component. Although this thesis has proposed that data exclusivity actually provides a limitation on the potentially perpetual secrecy of confidential information, this approach to the purpose of data exclusivity may provide little consolation in practice since longer periods of data exclusivity protection do contribute to delays in the market entry of cheaper, generic drugs. These delays result in the monopoly of more expensive medications, which affects access to affordable medicines and thus constitutes a public health issue. Perhaps owing to this reality, Mandamin J. made the following observation:

⁴³⁹ *Ibid* at para 127, citing Binnie J. in *Bristol-Myers Squibb Co v Canada (Attorney General)*, 2005 SCC 26, [2005] 1 SCR 533 at para 22. The *Bristol-Meyers* case mainly concerned the issuance of an NOC under the *Patented Medicines (Notice of Compliance) Regulations*, SOR/93-133 with respect to a drug from a different botanical source. This case was also decided prior to the 2006 amendments to the DPR.

⁴⁴⁰ See Lietzan, “Myths”, *supra* note 285 at 106.

⁴⁴¹ Recall from the discussion in section 2.1.5 that the public interest element in patent protection, namely the disclosure of information contained in the patent application, thereby constitutes the “bargain” in exchange for a limited term monopoly. However, as discussed in section 2.1.6, confidential information does not become public knowledge and also has the potential to remain forever secret. This lack of contribution to public knowledge accordingly results in an absence of an apparent public interest aspect with respect to the protection of confidential information.

The *Data Protection Regulation* does not directly add to public safety since it postpones the introduction of lower cost generic drugs. The [Regulatory Impact Analysis Statement] states that the *Data Protection Regulation* is to encourage innovator drug manufacturers, or at least allow them to recover their investment, and thereby foster innovators to develop new drugs. However, the evidence on this point is more of a logical assertion than a clear demonstration that innovators are not or will not bring forward new drugs for approval without the provision [emphasis added].⁴⁴²

The connection between data exclusivity and protection of the public health may be only theoretical. Nevertheless, perhaps there is merit in the argument that intellectual property rights enforcement is highly influential, if not outright determinative, in choosing the appropriate location for pharmaceutical research and development. For example, Michael Ravvin has noted that of the 1,556 new drugs that received market approval during the period from 1975 to 2004, only 21 drugs (barely greater than 1% of the total), targeted “neglected” tropical diseases.⁴⁴³ Ravvin has also observed that pharmaceutical research and development is devoted almost exclusively to diseases prevalent in affluent countries, because innovative companies have no incentive to invest in research and development in poor countries that cannot support monopoly drug prices.⁴⁴⁴

Mandamin J. observed that protecting public health and safety is a valid exercise of the federal government’s criminal law power, and that the regulatory drug scheme in the *Food and Drug Regulations* was “unquestionably valid criminal law legislation.” The contravention of either the *Food and Drugs Act* or the *Food and Drug Regulations* can result in liability for penalties including fines and imprisonment:

Subject to sections 31.1, 31.2 and 31.4, every person who contravenes any of the provisions of this Act or of the regulations, or fails to do anything the person was

⁴⁴² *Canadian Generic FC*, *supra* note 430 at para 76.

⁴⁴³ Michael Ravvin, “Incentivizing Access and Innovation for Essential Medicines: A Survey of the Problem and Proposed Solutions” (2008) 1 *Pub Health Ethics* 110 at 112.

⁴⁴⁴ *Ibid.*

ordered to do by an inspector under section 25 or 27.2, is guilty of an offence and liable

(a) on summary conviction for a first offence to a fine not exceeding five hundred dollars or to imprisonment for a term not exceeding three months or to both and, for a subsequent offence, to a fine not exceeding one thousand dollars or to imprisonment for a term not exceeding six months or to both; and

(b) on conviction on indictment to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding three years or to both.⁴⁴⁵

However, notwithstanding that the overall regulatory scheme of drugs falls within federal authority, Mandamin J. concluded that the DPR was *not* a public safety provision and was thus not *intra vires* the federal law criminal powers. In particular, Mandamin J. observed that the regulation of drug marketing has a “very significant impact in the area of commerce.”⁴⁴⁶ Thus, according to Mandamin J., the dominant feature of the DPR was the balancing of commercial considerations between the protection of an innovative manufacturer’s investment in preparing an NDS and the approval of a generic manufacturer’s ANDS for a lower cost generic copy of the same drug.⁴⁴⁷ The public health and safety aspect of the DPR therefore constituted an “adjunct rather than integral” part of the overall regulatory scheme.⁴⁴⁸

Nevertheless, Mandamin J. upheld the DPR as a valid exercise of the section 91(2) regulation of trade and commerce.⁴⁴⁹ He noted that the DPR addresses a “genuine, national economic concern” because Canada’s implementation or failure to implement international trade agreements has a “national dimension that relates to Canada’s ability

⁴⁴⁵ *Food and Drugs Act*, *supra* note 208, s 31.

⁴⁴⁶ *Canadian Generic FC*, *supra* note 430 at para 61.

⁴⁴⁷ *Ibid* at para 83.

⁴⁴⁸ *Ibid*.

⁴⁴⁹ *Ibid* at para 97, referring to *Canadian National Transportation Ltd. v. Canada (Attorney General)*, [1983] 2 SCR 206: Five criteria for validity under the second branch of the federal trade and commerce power are: (1) the legislation is part of a general regulatory scheme; (2) the scheme is monitored by an overseeing agency; (3) the legislation is concerned with trade as a whole rather than a particular industry; (4) that the provinces jointly or severally would be constitutionally incapable of passing such an enactment; and (5) the failure to include one or more provinces in the legislative scheme would jeopardize the successful operation of the scheme in other parts of the country.

to participate in world trade.”⁴⁵⁰ Furthermore, Mandamin J. stated that provincial legislatures cannot enact legislation that delays the approval of generic drugs for the market place. Provincial government approval for drugs for the marketplace would seriously encroach on federal criminal law powers to prohibit the marketing of drugs unless they have proven to be safe and effective. Finally, Mandamin J. held that the Governor in Council was properly delegated the authority to enact regulations and did not have indeterminate regulatory power to do so. Rather, Parliament has restricted the scope of the Governor in Council’s authority to a narrow area, since section 30(3) of the *Food and Drugs Act* expressly refers only to Article 1711 of NAFTA and paragraph 3 of Article 39 under TRIPS. The pith and substance of the DPR thus constitutes the balance regarding the commercial considerations between innovative and generic manufacturers that arise from the implementation of TRIPS and NAFTA.

At the appellate level, the Federal Court of Appeal upheld the decision of Mandamin J.⁴⁵¹ However, Nadon J.A. disagreed with Mandamin J.’s characterization of the pith and substance of the DPR. Whereas Mandamin J. had previously concluded that the protection of public safety was ancillary to the regulatory scheme, Nadon J.A. arrived at the opposite conclusion and asserted that the DPR must be interpreted in the context of the *Food and Drug Regulations* and its enabling statute.⁴⁵² By granting innovative manufacturers an eight-year period of market protection, the DPR encourages research

⁴⁵⁰ *Ibid* at para 105.

⁴⁵¹ *Canadian Generic Pharmaceutical Assn v Canada (Minister of Health)*, 2010 FCA 334, [2012] 2 FCR 618, aff’g 2009 FC 725, 348 FTR 29 (Eng), leave to appeal to SCC refused, [2011] SCCA No 54 [Canadian Generic FCA].

⁴⁵² Interestingly, Mandamin J. also interpreted the DPR in light of the entirety of the regulatory scheme as provided by the *Food and Drugs Act* and the *Food and Drug Regulations* yet arrived at a completely different understanding of the purpose of the DPR.

and development for new drugs, which thereby constitutes a valid health and safety purpose. Nadon J.A. stated:

The true purpose of the DPR is not to balance the commercial interests of innovators and generic drug manufacturers, but rather to ensure that Canadians have reasonable access, at reasonable prices, to new, safe and effective drugs...the Regulations as a whole encourage the research and development of new medicines that save lives, prevent diseases, heal and cure and improve the health of Canadians, who can only benefit from the discovery and development of new medicines after the information and data generated in extensive pre-clinical and clinical trials demonstrate the “innovative drug’s” safety and efficacy to the satisfaction of the Minister. The DPR plays an important part in this regulatory scheme.⁴⁵³

This interpretation of the DPR’s purpose was directly referenced by Stratas J.A. in *Takeda Canada Inc. v. Canada (Minister of Health)* (“*Takeda*”).⁴⁵⁴ Though the dispute in *Takeda* concerned the interpretation of the term “innovative drug” rather than the DPR at large, and Stratas J.A. also delivered the dissenting judgment, it is nevertheless important to note his judicial interpretation of the DPR’s purpose, particularly since he linked data exclusivity protection of an innovator’s investment to the public interest. In doing so, he observed that many new, safe, and efficacious drugs are now readily available to the public. However, “invisible” to the public are the “years of financial investment, effort, research, and testing, all undertaken with no assurance of success,” in which the entire process is filled with economic, scientific, and regulatory risk.⁴⁵⁵ Since drug manufacturers wish to maximize profits, greater risks and smaller potential rewards decrease the likelihood that drug manufacturers will invest in research and development.⁴⁵⁶ Accordingly, one area of risk concerns the “valuable” data generated by innovative manufacturers: if data that is submitted for regulatory approval can

⁴⁵³ *Canadian Generic FCA*, *supra* note 451 at para 114.

⁴⁵⁴ 2013 FCA 13; leave to appeal to the SCC refused, (2013) 460 NR 399.

⁴⁵⁵ *Ibid* at para 78.

⁴⁵⁶ *Ibid* at para 79.

immediately be used by competitors in order to obtain their own market approval, “what is the incentive for the innovator to innovate, submit data, and bring new drugs to market?”⁴⁵⁷ Stratas J.A. concluded that data exclusivity promotes innovation by altering the “risk-reward equation” for the innovator, who is then encouraged to research, discover, and develop new drugs.

Since the public benefits from new ideas and inventions, Stratas J.A. observed that data exclusivity obligations under TRIPS and NAFTA ensure that the protection is only conferred upon “new” chemical entities.⁴⁵⁸ This perspective of Stratas J.A. appears to reflect the balance sought by intellectual property law: since data exclusivity protects confidential information, a limited term monopoly is given to an innovator or “first mover” in exchange for a temporary interruption in the flow of valuable information. Data exclusivity accordingly brings back the “bargain” into the protection of confidential information, since it represents a break in the permanence of the secrecy therein.

The decision of the Federal Court of Appeal in *Canadian Generic* and the dissenting opinion of Stratas J.A. in *Takeda*⁴⁵⁹ reiterate a common perspective of data exclusivity, in that data exclusivity protects investment and subsequently leads to economic reward, which in turn fosters the development and availability of life-saving drugs, thereby resulting in positive public health outcomes. Because data exclusivity protects confidential information, these views reflect the *theoretical* connection between data exclusivity and public welfare, in that the public’s initial exclusion from knowledge will ultimately result in a greater benefit than would have been obtained had the information been immediately available.

⁴⁵⁷ *Ibid* at para 80.

⁴⁵⁸ *Ibid* at para 82.

⁴⁵⁹ Stratas J.A. was also the only judge in *Takeda* who discussed the nature and purpose of data exclusivity.

Having now completed a discussion of both the legislative regulation of clinical trials and data exclusivity, this thesis will next consider personal data protection governing the health sector in Canada.

3.2. Personal Health Information Legislation: Controlling Information in the Health Context

Prior to the enactment of health-specific personal data protection legislation, it was possible for personal health information to be governed by two different regulatory standards, depending on whether the data was held by public or private sector organizations. In Ontario, for example, two public sector statutes, such as the *Freedom of Information and Protection of Privacy Act*⁴⁶⁰ and the *Municipal Freedom of Information and Protection of Privacy Act*,⁴⁶¹ have governed access and privacy of personal information held by public sector organizations since 1988 and 1992, respectively.⁴⁶² However, because of their “piecemeal approach,” these statutes did not offer clear, statutory rules with respect to the consistent treatment of health records that were held by health care institutions in Ontario.⁴⁶³

With respect to the private sector, the *Personal Information Protection and Electronic Documents Act*⁴⁶⁴ (“PIPEDA”) was passed in April 2000 by the federal government.⁴⁶⁵ Before January 2004, PIPEDA was limited in scope to organizations

⁴⁶⁰ *FIPPA*, *supra* note 98.

⁴⁶¹ RSO 1990, c M.56.

⁴⁶² Halyna Perun, Michael Orr & Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act* (Toronto: Irwin Law Inc, 2005) [Perun et al].

⁴⁶³ *Ibid* at 7.

⁴⁶⁴ *PIPEDA*, *supra* note 101.

⁴⁶⁵ Perun et al, *supra* note 462 at 11.

under federal jurisdiction, such as banks and airlines.⁴⁶⁶ As of January 1, 2004, PIPEDA began to apply to all organizations within the country that collected, used, or disclosed personal information, including personal health information, in the course of commercial activities.⁴⁶⁷ PIPEDA would apply to these organizations unless a province had enacted “substantially similar” legislation that was applicable to these organizations, and the federal government had ordered an exemption from PIPEDA.⁴⁶⁸

Uncertainty regarding the application of PIPEDA, based on the term “commercial activities,” created a lack of consistency in the framework of privacy standards across the health sector.⁴⁶⁹ Also, since PIPEDA had been originally enacted to address the needs of electronic commerce, stakeholders in the health sector were concerned about whether PIPEDA was sufficiently adequate to address the complexities of the health system.⁴⁷⁰

The rationale amongst various provinces for health-specific personal data protection arose out of the need to create a framework that facilitated consistent provision of health care. The federal government has noted that enacting “substantially similar” legislation to PIPEDA would “enable provinces [and] territories to regulate the personal information management practices of organizations operating within their borders and to

⁴⁶⁶ *Ibid.*

⁴⁶⁷ *Ibid.*

⁴⁶⁸ *Ibid.* See also *PIPEDA*, *supra* note 101, s 26(2)(b):

The Governor in Council may, by order, ... if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.

⁴⁶⁹ Perun et al, *ibid* at 13.

⁴⁷⁰ *Ibid* at 12-13. For example, Schedule 1 of *PIPEDA*, *supra* note 117 at s 4.3.6 states that organizations “should generally seek express consent when the information is likely to be considered sensitive.” Perun et al thus note that the Ontario Medical Association and the Ontario Hospitals Association considered that having express consent as a required norm would unduly restrain the provision of care by health care professionals, given the fact that personal health information is almost always considered to be sensitive.

minimize the imposition of a dual regulatory regime on these organizations.”⁴⁷¹ Where a province enacted private sector (including health-related) personal data protection legislation that the federal government does not deem “substantially similar” to PIPEDA, affected organizations must comply with both statutes: PIPEDA and the provincial enactment.

Ontario’s PHIPA was thus designed to address this duality of regulatory regimes: the federal government duly designated PHIPA as “substantially similar” to PIPEDA, and health information custodians⁴⁷² under PHIPA are expressly exempt from the application of Part 1 of PIPEDA.⁴⁷³ The *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* do not apply to personal health information in the custody or control of a health information custodian.⁴⁷⁴

Table 1 contains the Canadian jurisdictions that have enacted health-specific personal data protection and addresses whether these statutes have been deemed to be substantially similar to PIPEDA. In addition to Ontario’s PHIPA, health-specific personal data protection statutes from New Brunswick,⁴⁷⁵ Newfoundland and Labrador,⁴⁷⁶ and

⁴⁷¹ Canada Gazette, *Process for the Determination of “Substantially Similar” Provincial Legislation by the Governor in Council*, Part I, (22 September 2001) 135(38), 3618 at 3619.

⁴⁷² Health information custodians will be defined and discussed later in this chapter.

⁴⁷³ See *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399, s(1):

Any health information custodian to which the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule A, applies is exempt from the application of Part I of the *Personal Information Protection and Electronic Documents Act* in respect of the collection, use and disclosure of personal information that occurs within the Province of Ontario.

⁴⁷⁴ *PHIPA*, *supra* note 384, s 8(1):

Subject to subsection (2), the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* do not apply to personal health information in the custody or under the control of a health information custodian unless this Act specifies otherwise.

⁴⁷⁵ *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265.

⁴⁷⁶ *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72.

Nova Scotia⁴⁷⁷ have been deemed substantially similar to PIPEDA. As shown in Table 1, there are six provinces with health-specific personal data protection legislation that have not been deemed substantially similar to PIPEDA.

Table 1 - Jurisdictions with Health-Specific Personal Information Protection Legislation

Jurisdiction	Statute	Deemed Substantially Similar to PIPEDA?⁴⁷⁸
Alberta	<i>Health Information Act</i> , RSA 2000, c H-5.	No
Saskatchewan	<i>Health Information Protection Act</i> , SS 1999 c H-0.021.	No
Manitoba	<i>Personal Health Information Act</i> , CCSM 2005, c P33.5.	No
Ontario	<i>Personal Health Information Protection Act</i> , RSO 2004, c 3.	Yes
New Brunswick	<i>Personal Health Information Privacy and Access Act</i> , SNB 2009, c P-7.05.	Yes
Newfoundland & Labrador	<i>Personal Health Information Act</i> , SNL 2008, c P-7.01.	Yes
Nova Scotia	<i>Personal Health Information Act</i> , SNS 2010, c 41.	Yes
Prince Edward Island	<i>Health Information Act</i> , RSPEI 1988, c H-1.41. ⁴⁷⁹	No
Yukon	<i>Health Information Privacy and Management Act</i> , SY 2013, c 16.	No
Northwest Territories	<i>Health Information Act</i> , SNWT 2014, c 2.	No

⁴⁷⁷ *Personal Health Information Custodians in Nova Scotia Exemption Order* SOR/2016-62.

⁴⁷⁸ Where a statute has not been deemed substantially similar to PIPEDA, PIPEDA will continue to apply to organizations in that province with respect to personal health information. The organization in question must then comply with both PIPEDA and the personal health information statute.

⁴⁷⁹ Proclaimed in force on July 1, 2017. See: Legislative Assembly of Prince Edward Island, Office of the Information and Privacy Commissioner, online: <<http://www.assembly.pe.ca/index.php3?number=1013943>> (accessed August 28, 2017).

There remain three Canadian jurisdictions that have not enacted health-sector specific personal data protection legislation. Table 2 identifies these jurisdictions and the personal data protection statutes that apply to organizations in the public and private sectors with respect to the handling of personal health information. The private sector statutes from British Columbia⁴⁸⁰ and Quebec⁴⁸¹ have been deemed to be substantially similar to PIPEDA and organizations in these provinces are thereby exempt from the application of PIPEDA. As Table 2 shows, PIPEDA still applies to private sector organizations in Nunavut.

Table 2 - Personal Data Protection Law Applicable Where Jurisdiction Has No Health-Specific Statute

Jurisdiction	Private Sector Statute	Public Sector Statute
British Columbia ⁴⁸²	<i>Personal Information Protection Act</i> , SBC 2003, c 63.	<i>Freedom of Information and Protection of Privacy Act</i> , RSBC 1996, c 165.
Quebec ⁴⁸³	<i>An Act Respecting the Protection of Personal Information in the Private Sector</i> , RSQ 2005, c P-39.	<i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information</i> , RSQ 2005, c A-2.1.
Nunavut	<i>Personal Information Protection and Electronic Documents Act</i> , SC 2000, c 5.	<i>Access to Information and Protection of Privacy Act</i> , SNWT 1994, c 20.

⁴⁸⁰ See *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.

⁴⁸¹ See *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

⁴⁸² In British Columbia, the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38 governs the protection of personal health information in databases known as “health information banks.” This statute is not relevant to this thesis.

⁴⁸³ In Quebec, *An Act Respecting the Sharing of Certain Health Information*, CQLR c P-9.0001 establishes “information assets” which include a database, information system, telecommunications system, and technological infrastructure that allow the sharing of health information to improve the security and quality of health and social services. This statute is not relevant to this thesis.

The following sections of this chapter will explore the link between personal data protection and data exclusivity through an analysis of the legislatively mandated practices for clinical trials and through the determination of the personal data protection laws that apply to the relevant parties that are required to maintain records regarding clinical trial participants.

3.3. Linking Data Exclusivity to Personal Data Protection

Clinical trial data originates from patients and healthy volunteers who participate in clinical trials, in which raw data is collected during the following periods: a) first enrollment; b) the trial itself; and c) completion of the study.⁴⁸⁴ Raw data consists of observations about individual participants, which are collected for the study protocol or as part of routine care.⁴⁸⁵ These data may be in the form of measurements of participant characteristics including weight, blood pressure, or heart rate and they can also include a baseline description of the participant's medical history including: physical exam

⁴⁸⁴ Institute of Medicine, *supra* note 392 at 93. The Institute of Medicine is a U.S. organization, and this document is a U.S. publication. However, it is informative to an analysis of the conduct of clinical trials in Canada and the personal data protection issues that arise therein.

First, both regulatory health agencies of the U.S. and Canada (the FDA and Health Canada, respectively) are members of the non-profit International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH). Among other goals, the ICH seeks “to encourage the implementation and integration of common standards” with respect to the interpretation and application of technical guidelines and requirements for the registration of pharmaceutical products. See: International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Mission: Harmonisation for Better Health*, online: <<http://www.ich.org/about/mission.html>> (accessed June 14, 2017).

Second, this publication was issued in response to the increasingly common practice of publicly sharing clinical trial data, which is particularly relevant to personal data protection issues. Although this practice has been in place for over ten years in the U.S. and Europe, Health Canada only recently announced a similar initiative in March 2017: see, Health Canada, *Public Release of Clinical Information in Drug Submissions and Medical Device Applications*, (Ottawa: Health Canada, 2017) online: <<https://www.canada.ca/en/health-canada/programs/public-release-clinical-information-drug-submissions-medical-device-applications.html>> (accessed March 15, 2017). Therefore, Canada does not possess a comprehensive guidance such as the present publication with respect to clinical trial data and patient privacy issues.

⁴⁸⁵ Institute of Medicine, *ibid* at 97.

information; clinical laboratory results; genome sequences; procedure results; and self-reported data such as a person’s quality of life.⁴⁸⁶ During the course of the trial, the raw data is “abstracted, coded, and transcribed” into an analyzable set,⁴⁸⁷ which is eventually “locked” into a final data set in which no further changes may be made.⁴⁸⁸

Both the raw data and analyzable data sets ultimately constitute individual participant data.⁴⁸⁹ Some observations, such as imaging results from X-rays or magnetic resonance imaging, must be interpreted (or “abstracted”) by study investigators and entered into case report forms as transcribed narrative data or as coded data according to the requisite coding procedures – for example, men may be coded as “0” and women as “1.”⁴⁹⁰ In addition to physiological and clinical measures, it is also becoming increasingly common to collect other types of health information in clinical trials, such as sensor data from smartphone applications, consumer genomics data, and participant-reported outcomes.⁴⁹¹

The need for documentation of the vast amount of patient information collected in a clinical trial requires clinical trial sponsors to maintain detailed records with respect to a drug used in a clinical trial. According to section C.05.012(3)(d) of the *Food and Drug Regulations*:

The sponsor shall maintain complete and accurate records in respect of the use of a drug in a clinical trial, including...records respecting the enrolment of clinical trial subjects, including **information sufficient to enable all clinical trial subjects to be identified** and contacted in the event that the sale of the drug may

⁴⁸⁶ *Ibid.*

⁴⁸⁷ *Ibid* at 93.

⁴⁸⁸ *Ibid* at 99. If the trial is blinded, the treatment code file is typically merged with the locked, analyzable data set, such that the data will be unblinded to the investigators. Although a large percentage of analyzable data is never used, it consists of information such as participant characteristics and primary outcome, secondary and tertiary outcomes, adverse events data, and exploratory data.

⁴⁸⁹ *Ibid* at 93.

⁴⁹⁰ *Ibid* at 97.

⁴⁹¹ *Ibid.*

endanger the health of the clinical trial subjects or other persons [emphasis added].⁴⁹²

The connection between the legislative regimes of data exclusivity and personal data protection, at least with respect to the *Food and Drug Regulations*, largely depends on the phrase “information sufficient to enable all clinical trial subjects to be identified.” If patients can be re-identified from de-identified clinical trial data, this would suggest that personal health information protection laws would apply to the data. At first glance, one might think that section C.05.012(3)(d) merely mandates that a master list of all contact information for registered clinical trial participants must be retained, such that there is no need for examination of the clinical trial data itself. However, there is a problem with this interpretation, since the provision mandates that clinical trial participants must first be identified *and* then contacted. Furthermore, because the provision expressly mentions that identification and contact are to occur *in the event that the drug would endanger participants’ health or that of others*, it would make little sense from a public health standpoint to contact individuals in a blind, wholesale manner, particularly since participants might have been randomized into multiple groups under different trial conditions and may require further medical intervention from having taken the experimental drug in the first place.

In mandating that individual clinical trial subjects be identifiable, section C.05.012 of the *Food and Drug Regulations* provides the strongest potential link between the legislative regimes of data exclusivity and personal data protection. Clinical trial data consists of an individual’s health information, and individuals have a right to control their

⁴⁹² *Food and Drug Regulations*, *supra* note 5, s C.05.012(3)(d).

personal information according to personal data protection laws.⁴⁹³ However, clinical trial sponsors maintain temporary, exclusive rights to clinical trial data because of federal data exclusivity legislation. This struggle over access to the same set of confidential information leads to a potential conflict with respect to Canada's abilities to comply with both data exclusivity and personal data protection obligations made internationally. To determine whether there is a conflict between these two regimes, the following issues will be addressed in this chapter: a) the definition of "personal health information" under provincial health information protection legislation; and b) whether clinical trial data retains the characteristics of information that constitutes "personal health information." In addition to clarifying the consistency of operation between data exclusivity and personal data protection, this analysis will help to determine the extent of rights of individual clinical trial participants to control their personal health information.

3.3.1. Record-Keeping Requirements: Good Clinical Practices and Identification of Patients

As mentioned in Chapter One, Canada's federal health regulatory agency, Health Canada, is a standing regulatory member of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use ("ICH").⁴⁹⁴ The ICH is a non-profit organization that seeks to achieve greater harmonization in the interpretation and application of guidelines and requirements for pharmaceutical product registration

⁴⁹³ For example, an individual's consent is generally required for the collection, use, and disclosure of the individual's personal health information under Ontario's PHIPA: see *PHIPA*, *supra* note 384, s 29.

⁴⁹⁴ See Government of Canada, *International Council for Harmonisation (ICH)*, online: <<https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/applications-submissions/guidance-documents/international-conference-harmonisation.html>> [Gov't of Canada (ICH)].

and “contribute to the protection of public health.”⁴⁹⁵ This harmonization is achieved through the development of ICH Guidelines through a “scientific consensus” with regulatory and industry experts, in which the ICH asserts that the key to success of this process is “the commitment of the ICH regulators to implement the final Guidelines.”⁴⁹⁶ Health Canada accordingly claims to be “committed to the adoption and implementation of ICH guidance and standards,”⁴⁹⁷ which includes the ICH’s *Guideline for Good Clinical Practice* (“ICH-GCP”).⁴⁹⁸ Health Canada’s commitment is thus consistent with Canada’s *Food and Drug Regulations*, which defines “good clinical practices” as “generally accepted practices that are designed to ensure the protection of the rights, safety, and well-being of clinical trial subjects and other persons.”⁴⁹⁹

Health Canada’s own *Guidance for Records Related to Clinical Trials* (“*Guidance*”) on the interpretation of the record-keeping requirement under section C.05.012 of the *Food and Drug Regulations* is directly influenced by the ICH-GCP.⁵⁰⁰ The ICH-GCP’s guidance contains a “minimum” list of “essential documents,” which constitutes an Annex to Health Canada’s *Guidance*. Importantly, some of these records are capable of identifying clinical trial participants. Table 3 describes these records, which are required to be kept by clinical trial sponsors and institutional investigators:

⁴⁹⁵ International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Mission: Harmonisation for Better Health*, online: <<http://www.ich.org/about/mission.html>> (accessed June 14, 2017).

⁴⁹⁶ *Ibid.*

⁴⁹⁷ See Gov’t of Canada (ICH), *supra* note 494.

⁴⁹⁸ International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice*, (9 November 2016), available online:

<http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6/E6_R2__Step_4.pdf> (accessed June 14, 2017) [ICH, “Clinical Practice”].

⁴⁹⁹ *Food and Drug Regulations*, *supra* note 5, s C.05.001.

⁵⁰⁰ Health Canada, *Guidance for Records Related to Clinical Trials: Interpretation of section C.05.012 of the Food and Drug Regulations - Division 5*, (May 23, 2006), online: <https://www.canada.ca/content/dam/hc-sc/migration/hc-sc/dhp-mps/alt_formats/hpfb-dgpsa/pdf/compl-conform/gui_68-eng.pdf> (accessed June 14, 2017) [Health Canada].

Table 3 - Required Records to be kept in the Course of Clinical Trials that can Identify Clinical Trial Subjects⁵⁰¹

Stage of Trial	Record Title	Record Purpose	Record Location (Files Of)	
			Investigator	Sponsor
During Clinical Phase	Source Documents	Documents the existence of the subject and substantiates the integrity of trial data collected – should include original documents related to the trial, to medical treatment, and history of subject	X	
	Subject Screening Log	Documents identification of subjects who entered pre-trial screening	X	X
	Subject Identification Code List	To document that the investigator or institution keeps a confidential list of names of all subjects allocated to trial numbers on enrolling in the trial. Allows investigator or institution to reveal the identity of any subject	X	
	Subject Enrollment Log	Documents chronological enrollment of subjects by trial number	X	
Completion or Termination of Trial	Completed Subject Identification Code List	Enables identification of all subjects enrolled in the trial in case a follow-up is necessary. List should be kept confidential and for an “agreed upon time”	X	
	Clinical Study Report	To document results and interpretation of the trial	X	X

⁵⁰¹ The contents of Table 3 have been adapted from “Essential Documents for the Conduct of a Clinical Trial”: ICH, “Clinical Practice”, *supra* note 498.

Based on Table 3, there would be at least the above records extant in every clinical trial. As will be demonstrated, personal data protection would give rights to patients in respect of each of these records.

The *Food and Drug Regulations* define a “sponsor” as an “individual, corporate body, institution, or organization that conducts a clinical trial,”⁵⁰² and sponsors are ultimately responsible for conducting trials in accordance with good clinical practices, which includes fulfilling the requirements with respect to information and records under section C.05.012 of the *Food and Drug Regulations*.⁵⁰³ Health Canada further clarifies the role of the sponsor as an individual, institution, or organization that is responsible for the “initiation, management, and/or financing of a clinical trial.”⁵⁰⁴ Sponsors also delegate many functions to third parties, including qualified investigators.⁵⁰⁵

The *Food and Drug Regulations* define a “qualified investigator” as “a person responsible to the sponsor for the conduct of the clinical trial at a clinical trial site, who is entitled to provide health care under the laws of the province where that clinical trial site is located.”⁵⁰⁶ Moreover, the person must be “a physician and a member in good standing of a professional medical or dental association.”⁵⁰⁷ Under the Health Canada *Guidance*, qualified investigators are required to retain clinical trial participants’ medical records as well as records that identify the participants.⁵⁰⁸

⁵⁰² *Food and Drug Regulations*, *supra* note 5, s C.05.001.

⁵⁰³ *Ibid*, s C.05.010 (i).

⁵⁰⁴ Health Canada, *supra* note 500 at 7. In the event that an independent investigator initiates a clinical trial under his or her own sponsorship, that investigator is responsible for all aspects of the trial as both a qualified investigator and a sponsor (see page 4).

⁵⁰⁵ *Ibid* at 9.

⁵⁰⁶ *Food and Drug Regulations*, *supra* note 5, s C.05.001.

⁵⁰⁷ *Ibid*. The person must be a physician or dentist for clinical trials for drugs used for dental purposes only. For all other cases, the person must be a physician.

⁵⁰⁸ Health Canada, *supra* note 500 at 9.

Table 3 indicates that some records that facilitate the identification of clinical trial subjects, such as the “completed subject identification code list,” are to be retained exclusively by the investigator rather than the sponsor. Based on this delegation of record retention, it may initially seem that only the qualified investigator is able to identify study participants. However, section C.05.012 of the *Food and Drug Regulations* expressly states that it is the *sponsor* that is responsible for the maintenance of records that would enable the identification of clinical trial participants. The Health Canada *Guidance* acknowledges that it is ultimately the sponsor’s responsibility to comply with the *Food and Drug Regulations*, and that in the event of any inconsistency or conflict with the *Food and Drug Regulations*, these regulations take precedence over the Health Canada *Guidance*.⁵⁰⁹ In this way, to comply with the *Food and Drug Regulations*, it follows that the sponsor must also retain the information that facilitates the identification of individual participants.

According to the ICH’s *Structure and Content of Clinical Study Reports* (“ICH-CSR”), a “clinical study report” (CSR) is a comprehensive report that integrates numerous pieces of information relating to an individual study of a drug or treatment conducted in patients.⁵¹⁰ Although the precise contents of a CSR may depend on the individual trial,⁵¹¹ the report is generally supposed to include information pertaining to treatment administered, selection of the study population, statistical analyses regarding efficacy, and safety evaluation. In particular, the ICH recommends that the CSR should

⁵⁰⁹ *Ibid* at 4.

⁵¹⁰ International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Structure and Content of Clinical Study Reports* (30 November 1995) at 1, online: <http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E3/E3_Guideline.pdf> (accessed June 14, 2017) [ICH, “Study Reports”].

⁵¹¹ *Ibid* at 2: This guideline states that “each report should consider all of the topics described (unless clearly not relevant) although the specific sequence and grouping of topics may be changed.”

describe demographic and other predictive characteristics of the study population, “and where the study is large enough to permit this, present data for demographic (e.g. age, sex, race, weight) and other (e.g. renal or hepatic function) subgroups” in order to identify possible differences in safety and efficacy.⁵¹² For example, the ICH-CSR recommends that the CSR include a listing of all patients discontinued from the study after enrolment, “broken down by centre and treatment group, giving a patient identifier, the specific reason for discontinuation, the treatment (drug and dose), cumulative dose, (where appropriate), and the duration of treatment before discontinuation.”⁵¹³ In addition, the ICH-CSR states that “it may also be useful to include information, such as critical demographic data (e.g. age, sex, race), concomitant medication, and the major response variable(s) at termination.”⁵¹⁴

The ICH-CSR notes that investigators should present and compare group data for “critical demographic and baseline characteristics of the patients,” and should also include a diagram that shows the relationship between the entire sample and any other groups in the analysis.⁵¹⁵ The ICH-CSR notes that the “critical” baseline variables in the group data will depend on the nature of the disease and protocol but will usually include demographic variables such as age, sex, race, as well as “disease factors” such as disease duration, stage, and severity, concomitant illness at trial initiation (e.g. renal disease, diabetes, heart failure), relevant previous illness, and relevant previous treatment for

⁵¹² *Ibid.*

⁵¹³ *Ibid* at 12-13. Annex V of the ICH-CSR contains an example of such a patient listing, in which the patient “identifier” is a number. The sample listing also includes the last visit and concomitant medication.

⁵¹⁴ *Ibid* at 13.

⁵¹⁵ *Ibid* at 13-14.

illness treated in the study.⁵¹⁶ Other potentially relevant variables include factors such as smoking, alcohol intake, special diets, and menstrual status.⁵¹⁷

It is thus clear that a clinical trial involves the collection and use of a significant amount of patient health information. Figure 5 illustrates the flow of information with respect to clinical trial data and the patient data contained therein, thereby representing the reality that while clinical trial data is part of the realm of confidential information, this data ultimately originates from patient data.

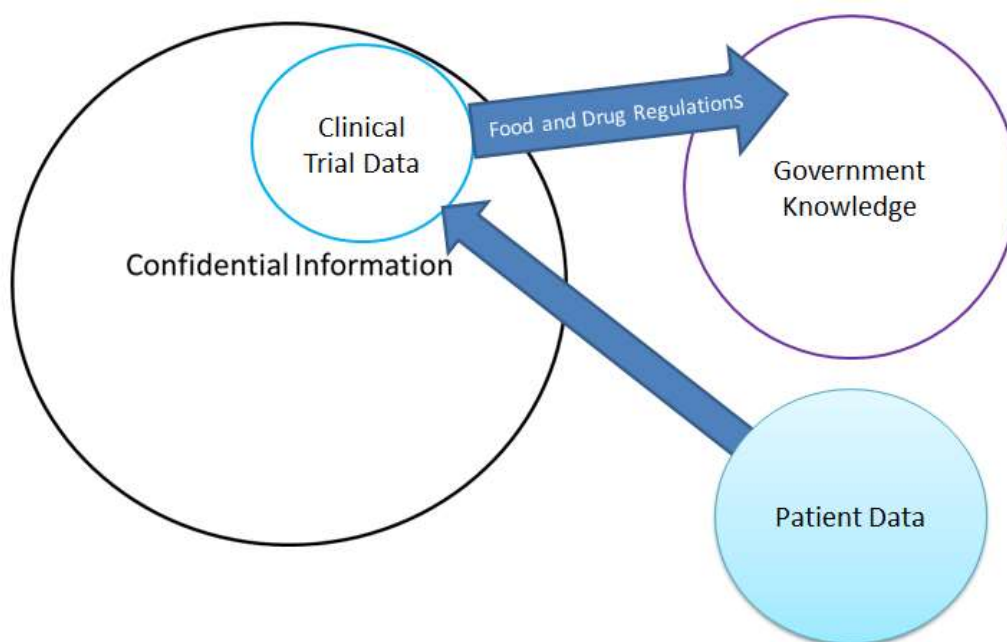


Figure 5 - Flow of Information with respect to Clinical Trial Data and Patient Data

This patient health information subsequently forms part of a CSR that is prepared in accordance with the ICH-CSR. Although the term “clinical study report” is not a defined term under the *Food and Drug Regulations*, sponsors are nonetheless required to submit, as part of regulatory market approval, “detailed reports of the tests made to

⁵¹⁶ *Ibid* at 14.

⁵¹⁷ *Ibid*.

establish the safety” with respect to an innovative drug’s recommended purpose and conditions of use.⁵¹⁸ The record-keeping requirements under section C.05.012 of the *Food and Drug Regulations* and the guidance prepared by the ICH and Health Canada also clearly indicate that patient identity is capable of being revealed at any time by both the sponsor and investigator alike despite the purported anonymization of patients through the assignment of code numbers.

There are two aspects of the personal data protection analysis that are important to determining whether there is a conflict between data exclusivity and personal data protection. First, in light of record-keeping requirements under the *Food and Drug Regulations* and Health Canada’s *Guidance*, one must determine the proper personal data protection legislation that applies to qualified investigators and clinical trial sponsors that possess the health information of clinical trial participants. Second, one must determine whether patient health information in clinical trial data constitutes *personal health information* within the meaning of personal health information protection laws or, where applicable, personal information within the meaning of public and private sector general personal data protection laws. As this thesis will show through a legislative analysis, patient health information that is collected and retained in clinical trials falls within the definition of identifiability under health-specific personal data protection statutes and also falls under the aegis, where applicable, of public and private sector general personal data protection laws. Therefore, personal data protection applies to clinical trial data. Furthermore, this thesis will also demonstrate that data exclusivity and personal data protection can operate consistently together in Canadian law.

⁵¹⁸ *Food and Drug Regulations*, *supra* note 5, s C.08.002 (2)(g).

3.3.2. Which Personal Data Protection Laws Apply to Qualified Investigators and Clinical Trial Sponsors?

The documentation and record-keeping responsibilities of the clinical trial sponsor and qualified investigator under Health Canada's *Guidance* and the *Food and Drug Regulations* are directly related to the application of the appropriate personal data protection laws. For example, in Ontario, section 29(1)(a) of PHIPA states that a "health information custodian" must not collect, use, or disclose an individual's personal health information unless "it has the individual's consent under this Act."⁵¹⁹ Section 3(1) of Ontario's PHIPA defines a "health information custodian" as follows:

"health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:

1. A health care practitioner or a person who operates a group practice of health care practitioners.
2. A service provider within the meaning of the *Home Care and Community Services Act, 1994* who provides a community service to which that Act applies.
3. A community care access corporation within the meaning of the *Community Care Access Corporations Act, 2001*.
4. A person who operates one of the following facilities, programs or services:
 - i. A hospital within the meaning of the *Public Hospitals Act*, a private hospital within the meaning of the *Private Hospitals Act*, a psychiatric facility within the meaning of the *Mental Health Act* or an independent health facility within the meaning of the *Independent Health Facilities Act*.
 - ii. A long-term care home within the meaning of the *Long-Term Care Homes Act, 2007*, a placement co-ordinator described in subsection 40 (1) of that Act, or a care home within the meaning of the *Residential Tenancies Act, 2006*.

⁵¹⁹ PHIPA, *supra* note 384, s 29(1)(a):

A health information custodian shall not collect, use or disclose personal health information about an individual unless...it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose.

ii.1 a retirement home within the meaning of the *Retirement Homes Act, 2010*.

iii. A pharmacy within the meaning of Part VI of the *Drug and Pharmacies Regulation Act*.

iv. A laboratory or a specimen collection centre as defined in section 5 of the *Laboratory and Specimen Collection Centre Licensing Act*.

v. An ambulance service within the meaning of the *Ambulance Act*.

vi. A home for special care within the meaning of the *Homes for Special Care Act*.

vii. A centre, program or service for community health or mental health whose primary purpose is the provision of health care.

5. An evaluator within the meaning of the *Health Care Consent Act, 1996* or an assessor within the meaning of the *Substitute Decisions Act, 1992*.

6. A medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act*.

7. The Minister, together with the Ministry of the Minister if the context so requires.

8. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons.⁵²⁰

Thus, in order for PHIPA to apply to an organization, the organization must be a “health information custodian” within the meaning of this definition. As mentioned previously in section 3.3 of this thesis, clinical trials involve the collection of a vast amount of personal health information from clinical trial participants, so it is important to clarify the responsibilities of the entities that will have custody and control over this information.⁵²¹ The question, then, is whether qualified investigators and clinical trial

⁵²⁰ *Ibid*, s 3(1).

⁵²¹ For example, see: Canadian Cancer Trials Group, *Privacy and Confidentiality* (October 1, 2015) at 6-7, available online: <<https://www.ctg.queensu.ca/docs/public/policies/PrivacyandConfidentiality.pdf>> (accessed August 6, 2017). This policy was released by the Canadian Cancer Trials Group (CCTG), a non-for-profit, non-government sponsor that develops and conducts clinical trials for the prevention and treatment of cancer. The policy expressly refers to PHIPA’s definition of health information custodians and

sponsors constitute health information custodians within the meaning of health-sector specific personal data protection statutes, such as PHIPA, and are thereby subject to the rules thereunder.

In Ontario, it is evident that qualified investigators constitute health information custodians under PHIPA. As mentioned previously, section C.05.001 of the *Food and Drug Regulations* mandates qualified investigators to be physicians. In Ontario, the practice of medicine is regulated under the *Medicine Act, 1991*,⁵²² which requires physicians to be members of the College of Physicians and Surgeons of Ontario.⁵²³ Under PHIPA, a health information custodian includes “a health care practitioner or a person who operates a group practice of health care practitioners,”⁵²⁴ in which a “health care practitioner” is defined as “a person who is a member within the meaning of the *Regulated Health Professions Act, 1991*⁵²⁵ and who provides health care.”⁵²⁶ The *Regulated Health Professions Act, 1991* defines a “member” as a “member of a College,”⁵²⁷ and includes medicine as a self-governing health profession under the *Medicine Act, 1991*.⁵²⁸ Since the *Regulated Health Professions Act, 1991* applies to any qualified investigator by virtue of his or her status as a physician, qualified investigators thus qualify as health information custodians within the meaning of PHIPA.

outlines the procedures for compliance with applicable personal data protection legislation and states that CCTG collects personal health information from participants who have provided written consent to participation in a clinical trial, including test results, adverse events, and medical history.

⁵²² SO 1991, c 30.

⁵²³ *Ibid*, s 9(3): “No person other than a member shall hold himself or herself out as a person who is qualified to practise in Ontario as an osteopath, physician or surgeon or in a specialty of medicine.” Section 1 of the *Medicine Act, 1991* defines “member” to mean “a member of the College,” in which “College” is defined as “the College of Physicians and Surgeons of Ontario.”

⁵²⁴ PHIPA, *supra* note 384, s 3.

⁵²⁵ SO 1991, c 18 [*Regulated Health Professions Act*].

⁵²⁶ PHIPA, *supra* note 384, s 2.

⁵²⁷ *Regulated Health Professions Act, supra* note 525, s 1(1).

⁵²⁸ *Ibid*, Sch 1.

It is also possible for clinical trials sponsors to qualify as health information custodians under PHIPA. Under Health Canada's *Guidance* with respect to record-keeping requirements, "independent investigators" who initiate a clinical trial under their own sponsorship become responsible for all aspects of that trial, both as a qualified investigator and a sponsor.⁵²⁹ In this way, clinical trial sponsors can be health information custodians under PHIPA if they are also qualified investigators, based on the requirement that a qualified investigator must be a physician.

However, it is less clear whether clinical trial sponsors that are businesses, such as pharmaceutical companies, constitute health information custodians within the meaning of health-sector specific statutes such as PHIPA. A corporate entity such as Merck Frosst, for example, is not encompassed⁵³⁰ by the above definition of a health information custodian under PHIPA. This exclusion reflects the fact that, while the research and development of life-saving drugs is directly relevant to human health outcomes, an entity such as Merck Frosst does not provide health care but engages in pharmaceutical innovation for the purpose of selling the products for profit. In other words, the activities of innovative pharmaceutical companies are better characterized as having a commercial or business purpose rather than a health care purpose.

Even if PHIPA does not apply to pharmaceutical companies such as Merck Frosst, these organizations are nonetheless governed by PIPEDA in the course of their commercial activities. So long as information pertains to an *identifiable* individual,⁵³¹ a

⁵²⁹ Health Canada, *supra* note 500 at 4.

⁵³⁰ According to *PHIPA*, *supra* note 384, s 2: "'prescribed' means prescribed by the regulations made under this Act." Pharmaceutical companies are not prescribed under PHIPA's General Regulation: see *Ontario Regulation*, 329/04.

⁵³¹ *PIPEDA*, *supra* note 101, s 2(1):

personal information means information about an identifiable individual [emphasis in original].

pharmaceutical company will be obligated to protect this information with respect to its collection, use, or disclosure in the course of commercial activities.⁵³² The Federal Court of Appeal in *Wyndowe v. Rousseau*⁵³³ observed that the definition of personal information under PIPEDA rendered this statute “very far reaching.”⁵³⁴ This interpretation is supported by Principle 4.9.1 under PIPEDA, which addresses access to personal information: since “organizations may choose to make sensitive medical information available through a practitioner,” Décary J.A. noted that “medical information”, which is “personal health information”, is “personal information.”⁵³⁵ PIPEDA also provides a definition of personal health information,⁵³⁶ and Décary J.A. asserted that, despite the fact that these expressions are defined “without reference to one another, it is clear that “personal health information” is a subset of “personal information.””⁵³⁷

⁵³² *Ibid*, s 4(1)(a): This Part applies to every organization in respect of personal information that...the organization collects, uses or discloses in the course of commercial activities.

⁵³³ *Wyndowe v Rousseau*, 2008 FCA 39, 373 NR 301 [*Wyndowe*].

⁵³⁴ *Ibid* at para 40.

⁵³⁵ *Ibid* at para 44, referring to *PIPEDA*, *supra* note 101, Sch 1, s 4.9.1.

⁵³⁶ *PIPEDA*, *supra* note 101, s 2(1):

personal health information, with respect to an individual, whether living or deceased, means

- (a) information concerning the physical or mental health of the individual;
- (b) information concerning any health service provided to the individual;
- (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- (d) information that is collected in the course of providing health services to the individual; or
- (e) information that is collected incidentally to the provision of health services to the individual [emphasis in original].

See also *Wyndowe*, *supra* note 533 at para 43: Décary J.A. observes that the only other place in PIPEDA in which “personal health information” is mentioned is at subsection 30(1.1), which is a transitional provision intended to delay the application of PIPEDA to “personal health information” until one year after section 30 comes into force. Décary J.A. states that the presumed reason for the delay was to allow practitioners who were about to be covered under PIPEDA to prepare for its application.

⁵³⁷ *Wyndowe*, *ibid* at para 42.

As mentioned previously, British Columbia,⁵³⁸ Quebec,⁵³⁹ and Alberta⁵⁴⁰ have enacted their own private sector personal data protection statutes which have all been deemed to be substantially similar to PIPEDA.⁵⁴¹ Accordingly, in their respective provinces, these private sector statutes would govern clinical trial sponsors that are pharmaceutical companies, replacing PIPEDA.⁵⁴²

Therefore, although personal health information is part of the data that is collected during clinical trials, the existence of health-specific personal data protection legislation in a jurisdiction does not necessarily mean that *all* parties involved in the clinical trial will be governed by this legislation. As discussed above, a “health information custodian” is a defined term under Ontario’s PHIPA, and pharmaceutical companies are not encompassed by this definition and consequently are not subject to the rules under PHIPA.

To determine the applicable personal data protection laws in other Canadian jurisdictions with respect to clinical trial sponsors and qualified investigators, this thesis first focuses on the jurisdictions with health-sector specific personal data protection and then provides an analysis of the definitions of health information custodians in the health-

⁵³⁸ *BC PIPA*, *supra* note 105.

⁵³⁹ *QC Act*, *supra* note 100.

⁵⁴⁰ *AB PIPA*, *supra* note 104.

⁵⁴¹ See: *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220; and *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

⁵⁴² For example, recall that Alberta’s private sector statute replaces the application of PIPEDA in the province of Alberta. See *AB PIPA*, *supra* note 104, s 4(3)(f):

This Act does not apply to...health information as defined in the *Health Information Act* to which that Act applies.

However, pharmaceutical companies are excluded from the scope of application of the *Health Information Act*, since they do not qualify as “custodians”: see Alberta’s *Health Information Act*, RSA 2000, c H-5, s 1(1)(f) [*AB HIA*] and *Health Information Regulation*, Alta Reg 70/2001, at s 2(2) [*AB Reg*]. Therefore, Alberta’s private sector statute applies to pharmaceutical companies that are clinical trial sponsors.

specific personal data protection statutes for the following jurisdictions: Alberta;⁵⁴³ Saskatchewan;⁵⁴⁴ Manitoba;⁵⁴⁵ New Brunswick;⁵⁴⁶ Newfoundland and Labrador;⁵⁴⁷ Nova Scotia;⁵⁴⁸ Prince Edward Island;⁵⁴⁹ Yukon;⁵⁵⁰ and the Northwest Territories.⁵⁵¹

Despite variations in the legislative definitions of health information custodians with respect to the institutions and individuals encompassed therein, health care providers constituted health information custodians in *all* these jurisdictions. Since health care providers are health information custodians within the meaning of health-specific personal data protection statutes, and in light of the requirement under the *Food and Drug Regulations* that a qualified investigator must be a physician,⁵⁵² Table 4 demonstrates that health-specific personal data protection applies to all qualified investigators in each of these jurisdictions but not to clinical trial sponsors in any of these jurisdictions. Clinical trial sponsors are instead governed by PIPEDA in each of these jurisdictions, except in Alberta, where Alberta's private sector legislation replaces the application of PIPEDA.⁵⁵³

⁵⁴³ See *AB HIA*, *ibid*, s 1(1)(f) and *AB Reg*, *ibid*, s 2.

⁵⁴⁴ The term "trustee" is used instead of "custodian": See *Health Information Protection Act*, SS 1999 c H-0.02, s 2(t) [*SK HIPA*], and *Health Information Protection Regulations*, RRS c H-0.021 Reg 1, s 3.

⁵⁴⁵ The term "trustee" is used instead of "custodian": See *Personal Health Information Act*, CCSM 2005, c P33.5, s 1(1) [*MB PHIA*].

⁵⁴⁶ See *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s 1 [*NB PHIPAA*], and *General Regulation*, NB Reg 2010-112, s 3.

⁵⁴⁷ See *Personal Health Information Act*, SNL 2008, c P-7.01, s 4 [*NL PHIA*], and *Personal Health Information Regulations*, NLR 38/11, s 4.

⁵⁴⁸ See *Personal Health Information Act*, SNS 2010, c 41, s 3(f) [*NS PHIA*], and *Personal Health Information Regulations*, NS Reg 217/2012, s 3.

⁵⁴⁹ See *Health Information Act*, RSPEI 1988, c H-1.41, s 1(e) [*PEI HIA*].

⁵⁵⁰ See *Health Information Privacy and Management Act*, SY 2013, c 16, s 2(1) [*YK HIPMA*] and *Health Information General Regulation*, YOIC 2016/159, s 3.

⁵⁵¹ See *Health Information Act*, SNWT 2014, c 2, s 1(1) [*NT HIA*], and *Health Information Regulations*, NWT Reg 089-2015, s 1(1).

⁵⁵² *Food and Drug Regulations*, *supra* note 5, s C.05.001.

⁵⁵³ Alberta's private sector statute applies to pharmaceutical companies that are clinical trial sponsors. First, recall that Alberta's private sector statute replaces the application of PIPEDA in the province of Alberta by virtue of having been deemed substantially similar to PIPEDA. Alberta's private sector statute also does not apply to information under Alberta's *Health Information Act*: see *AB PIPA*, *supra* note 104, s 4(3)(f):

Table 4 - Application of Health-Specific Personal Data Protection in Clinical Trials

Jurisdiction	Applies to Qualified Investigator (Physician)?	Applies to Clinical Trial Sponsor (Business – i.e. Pharmaceutical Company)?
Alberta	Yes	No; the <i>Personal Information Protection Act</i> applies
Saskatchewan	Yes	No; PIPEDA applies
Manitoba	Yes	No; PIPEDA applies
Ontario	Yes	No; PIPEDA applies
New Brunswick	Yes	No; PIPEDA applies
Newfoundland and Labrador	Yes	No; PIPEDA applies
Nova Scotia	Yes	No; PIPEDA applies
Prince Edward Island	Yes	No; PIPEDA applies
Yukon	Yes	No; PIPEDA applies
Northwest Territories	Yes	No; PIPEDA applies

British Columbia, Quebec, and Nunavut have been excluded from Table 4 since none of these jurisdictions has enacted a health-specific personal data protection statute. Table 5 identifies the applicable personal data protection laws with respect to qualified investigators and clinical trial sponsors in these jurisdictions. The public sector personal data protection statutes in these jurisdictions apply to qualified investigators that are in possession of health information.⁵⁵⁴ The private sector statutes in British Columbia⁵⁵⁵ and

This Act does not apply to...health information as defined in the *Health Information Act* to which that Act applies.

However, pharmaceutical companies are excluded from the scope of application of the *Health Information Act*, since they do not qualify as “custodians”: see *AB HIA*, *supra* note 542, s 1(1)(f) and *AB Reg*, *supra* note 542, s 2(2).

⁵⁵⁴ The application of public sector legislation to qualified investigators in this context assumes that these physicians are operating within public organizations, such as hospitals.

⁵⁵⁵ See *BC PIPA*, *supra* note 105, s 3: British Columbia’s private sector statute applies to “every organization” but does not apply where British Columbia’s public sector statute, the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, applies to personal information.

Quebec⁵⁵⁶ replace the application of PIPEDA in governing clinical trial sponsors in these provinces, and PIPEDA will continue to apply to clinical trial sponsors in Nunavut.

Table 5 - Application of Personal Data Protection in Clinical Trials for Jurisdictions without Health-Sector-Specific Statutes

Jurisdiction	Qualified Investigator (Physician)	Clinical Trial Sponsor (Business – i.e. Pharmaceutical Company)
British Columbia	<i>Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.</i>	<i>Personal Information Protection Act, SBC 2003, c 63.</i>
Quebec	<i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, RSQ. 2005, c A-2.1.</i>	<i>An Act Respecting the Protection of Personal Information in the Private Sector, RSQ, c P-39.</i>
Nunavut	<i>Access to Information and Protection of Privacy Act, SNWT 1994, c 20.</i>	<i>Personal Information Protection and Electronic Documents Act, SC 2000, c 5.</i>

In determining which personal data protection laws that apply to the relevant entities holding patient health information, it was necessary to first identify whether these entities fell within the definition of information “custodian”: if they do, they lie within the scope of health-specific personal data protection statutes. In all cases, the qualified investigator under the clinical trials regime falls within this scope where there is applicable health-sector specific legislation (see Table 4). Where there is no such legislation, the qualified investigator is governed by the relevant public sector personal data protection statutes (see Table 5). In the case of clinical trial sponsors, because they

⁵⁵⁶ See *QC Act, supra* note 100, s 1: The purpose of this statute is to establish rules concerning the protection of personal information which a person “collects, holds, uses, or communicates...in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code.” See also: *Civil Code of Quebec, CQLR c CCQ-1991, art 1525*, which defines an enterprise as “the carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service.”

are purely businesses, private sector personal data protection legislation (either provincial or PIPEDA) will apply rather than health-specific or public sector personal data protection.

The following section of this thesis will explore the definition of “personal health information” with respect to the concept of identifiability of the individual and how the application of personal data protection laws affects individuals’ rights to control their personal health information in the context of data exclusivity.

3.4. What Information Qualifies as “Personal Health Information”⁵⁵⁷ under Canadian Legislation?

3.4.1. The Notion of Identifiability

Consider the famous anecdote about the priest who was asked, at a party, whether he had heard any exceptional stories during confessionals. “In fact,” the priest replied, “my first confessor is a good example, since he confessed to a murder.” A few minutes later, an elegant man joined the group, saw the priest, and greeted him warmly. When asked how he knew the priest, the man replied: “Why, I had the honor of being his first confessor.”⁵⁵⁸

This anecdote, offered by Ruth Gavison, illustrates the need to clarify the notion of “identifiability” as it relates to the definition of personal information within the meaning of personal data protection laws. As the custodian of the information about the identity of the murderer, it is clear that the priest felt confident that, in withholding the confessor’s name, the sensitive information he did reveal was sufficiently anonymous as to safeguard the confessor’s identity. At the time of the priest’s disclosure, no one present could have uniquely identified the individual to whom the priest was referring. However, an additional piece of information that was later made available ultimately removed all doubts about the individual’s identity. Gratton also notes that, while information may not

⁵⁵⁷ Alberta uses the term “health information” instead of “personal health information.”

⁵⁵⁸ Ruth Gavison, “Privacy and the Limits of Law” (1980) 89 Yale LJ 421 at 430-431.

initially be “identifiable” within the meaning of personal data protection laws, acquiring a certain volume of information will eventually be sufficient to make that bundle of information “identifiable.”⁵⁵⁹

Clarification of the definition of identifiability can involve a factual determination of what it means to “de-identify” data, and whether such de-identification is sufficient to render it non-personal information and safeguard the identity of the confidante individual who confided the data. Data that has been de-identified can lead to later violations of patient privacy owing to re-identification through the proliferation of large-scale analyses of vast data sets.⁵⁶⁰ Solon Barocas and Helen Nissenbaum observe that the promise of anonymity is impossible to fulfil if individual records contain information that may fall outside the scope of the commonly defined set of personally identifiable information but nonetheless distinguish a person sufficiently to associate those records to a specific individual.⁵⁶¹ For example, combining an anonymized data set with a separate data set that includes identifying information, and subsequently looking for areas of overlap in the combined data, increases the likelihood of being able to re-identify individuals in the data set or determine whether they belong to a subgroup with certain attributes.⁵⁶² The existence of these techniques raises the issue of whether de-identified data sufficiently addresses the interests of individual patients in maintaining the confidentiality of their personal health information.

⁵⁵⁹ *Gratton, supra* note 406 at 184.

⁵⁶⁰ Institute of Medicine, *supra* note 392 at 53.

⁵⁶¹ Solon Barocas & Helen Nissenbaum, “Big Data’s End Run around Anonymity and Consent,” in Julia Lane et al, *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014), 44-75 at 50, available online: <
<https://www.nyu.edu/projects/nissenbaum/papers/BigDatasEndRun.pdf>>.

⁵⁶² *Ibid.*

The issue of identifiability is particularly relevant in the context of clinical trials with respect to the application of personal data protection laws because the ability to uniquely identify an individual is essential to the definition of personal information in both international instruments and Canadian legislation. The international OECD Privacy Guidelines define “personal data” as “any information relating to an identified or identifiable individual (data subject).”⁵⁶³ Similarly, Canada’s federal PIPEDA states that information about an “identifiable” individual constitutes personal information.⁵⁶⁴ Although neither the OECD Privacy Guidelines nor PIPEDA offer definitions of “identifiable,” Khaled El Emam et al have observed that information that permits the direct recognition of an individual, including personal names, social insurance numbers, and telephone numbers constitutes “direct identifiers.”⁵⁶⁵ In contrast, “quasi-identifiers” are characteristics that can indirectly identify individuals and include demographic and socioeconomic information such as a person’s date of birth, ethnicity, and income level.⁵⁶⁶

The identifiability of an individual is also an essential characteristic of personal information in the health context. For example, section 4 of Ontario’s PHIPA defines personal health information to mean “identifying information about an individual” with respect to several features that include the individual’s physical or mental health, family health history, and health number.⁵⁶⁷ “Identifying information” is defined under PHIPA

⁵⁶³ *OECD Guidelines*, *supra* note 92, s 1(b).

⁵⁶⁴ See *PIPEDA*, *supra* note 101, s 2(1).

⁵⁶⁵ Khaled El Emam, Sam Rodgers & Bradley Malin, “Anonymizing and Sharing Individual Patient Data” (2015) 350 *BMJ* 1-5 at 2 [El Emam et al].

⁵⁶⁶ *Ibid* at 2.

⁵⁶⁷ *PHIPA*, *supra* note 384, s 4(1):

“personal health information”, subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,

as information that identifies an individual or that could be used to identify an individual.⁵⁶⁸ Since identifying information includes that which *could be used to identify an individual*, Ontario's PHIPA appears to contemplate situations in which information could be used in combination with other information to identify an individual.

Recall from section 3.3.2 of this thesis that it was essential to determine the relevant personal data protection laws applying to the qualified investigators and clinical trial sponsors that have custody of personal health information in clinical trials in order to clarify their responsibilities in protecting this information. It is now important to determine whether the information involved constitutes information about an “identifiable” individual: since identifiability is a key aspect of the definition of personal health information, information that does not qualify as identifiable would be excluded from the scope of the definition, which could subsequently affect the responsibilities of those who have custody of the information. In this context, understanding of the “identifiability” of information is a key determinant for whether there is a conflict between data exclusivity and personal data protection. If personal data protection does not apply because there is no personal health information in clinical trial data by the time

-
- (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
 - (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
 - (c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
 - (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
 - (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
 - (f) is the individual's health number, or
 - (g) identifies an individual's substitute decision-maker.

⁵⁶⁸ *Ibid.*, s 4(2): PHIPA defines ““identifying information” as “information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.”

data exclusivity law applies, then there is no conflict between the legislative regimes of personal data protection and data exclusivity.

3.4.2. Identifiability of the Individual: Application of Personal Data Protection and Control over Information

The precise definitions of personal health information differ between jurisdictions. For example, Manitoba's personal health information statute has been in force since 1997, and offers the following definition of personal health information:

- “personal health information” means recorded information about an identifiable individual that relates to
- a) the individual's health, or health care history, including genetic information about the individual,
 - b) the provision of health care to the individual, or
 - c) payment for health care provided to the individual,
- and includes
- d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and
 - e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.⁵⁶⁹

Prince Edward Island is the most recent province to have enacted personal health information protection legislation. The *Health Information Act*⁵⁷⁰ received Royal Assent on May 14, 2014 and was proclaimed in force on July 1, 2017. In contrast with the legislation of Manitoba, Prince Edward Island's *Health Information Act* offers a more detailed description of the characteristics and activities that contribute to the definition of personal health information:

- “personal health information” means identifying information about an individual in oral or recorded form that
- (i) relates to the individual's physical or mental health, family health history or health care history, including genetic information about the individual,

⁵⁶⁹ *MB PHIA*, *supra* note 545, s 1(1).

⁵⁷⁰ *PEI HIA*, *supra* note 549.

- (ii) relates to information about an individual that is collected for the purpose of registering the individual for the provision of health care, including a health number, medical record number and any other identifier assigned to an individual,
- (iii) relates to the provision of health care to the individual,
- (iv) relates to an individual's entitlement to benefits under or participation in a health care program or service,
- (v) is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service,
- (vi) relates to a drug, a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care provider,
- (vii) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,
- (viii) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance,
- (ix) identifies the individual's substitute decision maker, or
- (x) identifies the individual's health care provider.⁵⁷¹

Of the ten Canadian jurisdictions with health-specific personal data protection, eight jurisdictions expressly include the notion of identifiability in their definition of personal health information. These include Ontario,⁵⁷² New Brunswick,⁵⁷³ Nova Scotia,⁵⁷⁴ Newfoundland and Labrador,⁵⁷⁵ Manitoba,⁵⁷⁶ Prince Edward Island,⁵⁷⁷ the Yukon,⁵⁷⁸ and the Northwest Territories.⁵⁷⁹ Whereas the legislation from Manitoba merely requires personal health information to relate to an “identifiable” individual,⁵⁸⁰ the statutes from Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia, Prince Edward Island, and the Yukon expressly define “identifying” information, and these definitions

⁵⁷¹ *Ibid*, s 1(t).

⁵⁷² See *PHIPA*, *supra* note 384, s 4(1).

⁵⁷³ See *NB PHIPAA*, *supra* note 546, s 1.

⁵⁷⁴ *NS PHIA*, *supra* note 548, s 3(r).

⁵⁷⁵ *NL PHIA*, *supra* note 547, s 5(1).

⁵⁷⁶ *MB PHIA*, *supra* note 545, s 1(1).

⁵⁷⁷ *PEI HIA*, *supra* note 549, s 1(t).

⁵⁷⁸ *YK HIPMA*, *supra* note 550, s 2(1).

⁵⁷⁹ *NT HIA*, *supra* note 551, s 1(1).

⁵⁸⁰ *MB PHIA*, *supra* note 545, s 1(1).

are essentially identical in each jurisdiction.⁵⁸¹ For example, New Brunswick's *Personal Health Information Privacy and Access Act* describes "identifying information" as follows:

"identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.⁵⁸²

One thus observes that, in addition to being able to *directly* identify an individual, identifying information also constitutes that for which identification of the individual is *likely* to occur. Moreover, the definition of identifying information also contemplates the possibility of information being combined with other data in order to render the individual capable of being identified.

The statutory definitions of identifying information in health-specific personal data protection thus support the proposition that personal data protection applies to clinical trial data, despite the removal of direct identifiers such as a participant's name. To use New Brunswick's personal health information protection legislation as an example, "identifying information" includes information "*for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual* [emphasis added]."⁵⁸³ Recall that, in accordance with good clinical practices and the *Food and Drug Regulations*,⁵⁸⁴ qualified investigators and clinical trial sponsors are required to maintain certain records in a

⁵⁸¹ See *PHIPA*, *supra* note 384, s 4(2); *NB PHIPAA*, *supra* note 546, s 1; *NL PHIA*, *supra* note 547, s 5(5); *NS PHIA*, *supra* note 548, s 3(1); *PEI HIA*, *supra* note 549, s 1(o); *YK HIPMA*, *supra* note 550, s 2(1). See also, *NT HIA*, *supra* note 551, s 1(1): the statute from the Northwest Territories does not offer a definition of "identifying information" but instead directly includes a description of identifiability in its definition of personal health information: personal health information constitutes information which "identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual."

⁵⁸² *NB PHIPAA*, *supra* note 546, s 1.

⁵⁸³ *Ibid.*

⁵⁸⁴ Please refer to the previous discussion in section 3.3.1 of this thesis.

clinical trial. For example, qualified investigators are required to keep a “Subject Identification Code List,” that would allow the investigator to reveal the identity of any subject⁵⁸⁵ and clinical trial sponsors must maintain “*information sufficient to enable all clinical trial subjects to be identified* and contacted in the event that the sale of the drug may endanger the health of the clinical trial subjects or other persons [emphasis added].”⁵⁸⁶ In New Brunswick, although clinical trial data may be transcribed and coded, such that one may not be able to *immediately* point to a particular individual, a participant’s health information in a clinical trial constitutes “identifying information” within the meaning of New Brunswick’s health information protection statute because it can be combined with other information, such as a “Subject Identification Code List,” in order to uniquely identify the individual.

The health-specific personal data protection statutes from Alberta⁵⁸⁷ and Saskatchewan⁵⁸⁸ do not refer to identifiability in their definitions of personal health information. However, Alberta’s *Health Information Act* is noteworthy because it identifies two categories of “health information.”⁵⁸⁹ “non-identifying” and “individually

⁵⁸⁵ Please refer to Table 3, above, which includes the Subject Identification Code List as an essential record that must be retained in a clinical trial, through which the identity of any clinical trial participant can be revealed.

⁵⁸⁶ *Food and Drug Regulations*, *supra* note 5, s C.05.012(3)(d).

⁵⁸⁷ See *AB HIA*, *supra* note 542, s 1(1)(k). Alberta uses the term “health information” instead of “personal health information.”

⁵⁸⁸ See *SK HIPA*, *supra* note 544, s 2(m).

⁵⁸⁹ Alberta’s health information protection statute, *AB HIA*, *supra* note 542, s 1(i) defines “diagnostic, treatment, and care information” as: “(i) the physical and mental health of an individual; (ii) a health service provided to an individual, including the following information respecting a health services provider who provides a health service to that individual...; (iii) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance; (iv) a drug as defined in the *Pharmacy and Drug Act* provided to an individual; (v) a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization; (vi) the amount of any benefit paid or payable under the *Alberta Health Care Insurance Act* or any other amount paid or payable in respect of a health service provided to an individual, and includes any other information about an individual that is collected when a health service is provided to the individual, but does not include information that is not written, photographed, recorded or stored in some manner in a record.” This definition is included as part of “health information,” under Alberta’s *Health*

identifying.” The term “non-identifying” with respect to describing health information means that “the identity of the individual who is the subject of the information cannot be readily ascertained from the information.”⁵⁹⁰ In contrast, ““individually identifying”, when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information.”⁵⁹¹ In light of the record-keeping requirements under the *Food and Drug Regulations* and the potential identification of an individual clinical trial participant in this manner, Alberta’s definition of “individually identifying” health information also supports the notion that its personal data protection applies to clinical trial data.

Recall that the previous analysis in section 3.3.2 found that clinical trial sponsors which are pharmaceutical companies would not be subject to health-specific personal data protection but would instead be governed by PIPEDA or, in British Columbia, Alberta, and Quebec, by the private sector statutes of those provinces. PIPEDA and the private sector statutes from British Columbia, Alberta, and Quebec all expressly state that “personal” information constitutes that which is about an identifiable individual.⁵⁹² These definitions of personal information and the potential for clinical trial sponsors to identify all participants in accordance with the record-keeping requirements under the *Food and Drug Regulations*⁵⁹³ are consistent with the proposition that personal data in clinical trials remains identifiable.

Information Act: “health information” means one or both of the following: (i) diagnostic, treatment and care information; (ii) registration information. See *AB HIA*, *supra* note 542, s 1(1)(k).

⁵⁹⁰ *Ibid.*, s 1(1)(r).

⁵⁹¹ *Ibid.*, s 1(1)(p).

⁵⁹² See *PIPEDA*, *supra* note 101, s 2(1); *BC PIPA*, *supra* note 105, s 1; *AB PIPA*, *supra* note 104, s 1(1)(k); *QC Act*, *supra* note 100, s 2, where “personal information” is that which relates to a natural person and allows that person to be identified.

⁵⁹³ See *Food and Drug Regulations*, *supra* note 5, s C.05.012(3)(d).

This thesis has thus found that all patient data in clinical trials in Canada is subject to personal data protection. All three constructs to be explored in addressing the research question of this thesis have now been analyzed: the legislative regulation of clinical trials, the data exclusivity right of pharmaceutical companies, and the individual's right to personal data protection. Having established the personal data protection applicable to health care settings in every province, and having explored the requirements for data exclusivity across Canada, the issue is whether there are situations in which personal information gathered during clinical trials ceases to be subject to personal data protection legislation. The following section explores this issue.

3.4.3. De-Identified Health Information: Definitions and Consequences of this Classification

Five of the ten personal health information protection statutes surveyed offer an express definition of de-identification of information. These jurisdictions are Saskatchewan,⁵⁹⁴ Ontario,⁵⁹⁵ New Brunswick,⁵⁹⁶ Nova Scotia,⁵⁹⁷ and Prince Edward Island.⁵⁹⁸ The provisions that define “de-identified information” differ slightly in language and degree of detail. New Brunswick's *Personal Health Information Privacy and Access Act* offers a broad definition of de-identification: when the term “de-

⁵⁹⁴ *SK HIPA*, *supra* note 544, s 2(d):

“de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed.

⁵⁹⁵ *PHIPA*, *supra* note 384, s 47(1):

“de-identify”, in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and “de-identification” has a corresponding meaning.

⁵⁹⁶ *NB PHIPAA*, *supra* note 546, s 1.

⁵⁹⁷ *NS PHIA*, *supra* note 548, s 3(g).

⁵⁹⁸ *PEI HIA*, *supra* note 549, s 1(g).

identified” is used to refer to personal health information, it means “personal health information from which all identifying information has been removed.”⁵⁹⁹

Saskatchewan’s statute also defines de-identified information in a broad manner but also contemplates the likelihood of identification of the individual, since “de-identified personal health information” means “personal health information from which any information that may reasonably be expected to identify an individual has been removed.”⁶⁰⁰ The de-identification definitions from Ontario and Nova Scotia contemplate the likelihood of identification and also consider the possibility that information can be used with other information in identifying the individual. According to Ontario’s PHIPA, to “de-identify” information means “to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.”⁶⁰¹ Similarly, Nova Scotia’s legislation defines “de-identified information,” as “information that has had all identifiers removed that identify the individual, or where it is reasonably foreseeable in the circumstances, could be utilized, either alone or with other information, to identify the individual.”⁶⁰² Finally, Prince Edward Island’s *Health Information Act* is the only legislation to refer to specific anonymization techniques in its definition of “de-identified information” as “personal health information that has been stripped, encoded or otherwise transformed so as to ensure that the identity of the individual who was the

⁵⁹⁹ *NB PHIPAA*, *supra* note 546, s 1.

⁶⁰⁰ *SK HIPA*, *supra* note 544, s 2(d).

⁶⁰¹ *PHIPA*, *supra* note 384, s 47(1). PHIPA offers this definition of de-identification for the purposes of section 47, entitled “Disclosure for analysis of health system.” However, the definition is nonetheless informative and provides insight into what constitutes identifying information.

⁶⁰² *NS PHIA*, *supra* note 548, s 3(g).

subject of the personal health information cannot be readily ascertained from the de-identified information.”⁶⁰³

Perhaps the difference in the language of these provisions reflects the reality that anonymization techniques are not standardized across jurisdictions. El Emam et al have noted that the concept of anonymous or non-identifiable data is ambiguous, which in turn contributes to heterogeneity and inconsistency in actual anonymization practices for health data.⁶⁰⁴ However, the robustness of anonymization merits close consideration since some legislators in the area of personal data protection seem to have depended upon de-identification techniques to deliver, as Paul Ohm expresses it, “the best of both worlds: the benefits of information flow and strong assurances of privacy.”⁶⁰⁵

Most important, characterizing information as “de-identified” leads to serious implications with respect to the breadth of activities that are authorized in relation to this information. Personal health information protection statutes from five Canadian jurisdictions expressly authorize the collection, use, and disclosure of de-identified information for *any* purpose: Alberta,⁶⁰⁶ New Brunswick,⁶⁰⁷ Prince Edward Island,⁶⁰⁸ the Yukon,⁶⁰⁹ and the Northwest Territories.⁶¹⁰ On the other hand, the statutes from

⁶⁰³ *PEI HIA*, *supra* note 549, s 1(g).

⁶⁰⁴ El Emam et al, *supra* note 575 at 1.

⁶⁰⁵ Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” (2010) 57 *UCLA L Rev* 1701 at 1704 at 1732 [Ohm].

⁶⁰⁶ See *AB HIA*, *supra* note 542, ss 19, 26 & 32 which authorize, respectively, the collection, use, and disclosure of “non-identifying” health information for “any purpose.”

⁶⁰⁷ See *NB PHIPAA* *supra* note 546, ss 30, 33 & 36 which authorize, respectively, the collection, use, and disclosure of “de-identified information” for “any purpose.”

⁶⁰⁸ See *PEI HIA*, *supra* note 549, ss 20, 22(4) & 23(4) which authorize, respectively, the collection, use, and disclosure of “de-identified” information for “any purpose.”

⁶⁰⁹ *YK HIPMA*, *supra* note 550, s 14:

Nothing in this Act limits any person’s right to collect, use or disclose information that is not identifying information.

⁶¹⁰ *NT*, *supra* note 551, s 1(4):

Nothing in this Act shall be construed so as to prevent a health information custodian from collecting, using, or disclosing non-identifying information.

Saskatchewan,⁶¹¹ Manitoba,⁶¹² New Brunswick,⁶¹³ Nova Scotia,⁶¹⁴ and Prince Edward Island⁶¹⁵ do not authorize collection, use, and disclosure for “any” purpose but instead expressly exclude de-identified information from the scope of their application. Although it may seem illogical for certain of these statutes, namely those from New Brunswick and Prince Edward Island, to exclude de-identified information from the scope of their application *while simultaneously* authorizing the collection, use, and disclosure of this de-identified information for any purpose, this situation merely means that de-identified information is not protected by the statutory rules limiting collection, use, and disclosure.

The legal authorization to collect, use, and disclose de-identified or anonymized health information for *any* purpose reflects the legislators’ apparent confidence in the factual robustness of anonymization as an adequate safeguard for individual privacy interests. In other words, for confidentiality to be upheld by de-identification, de-identified data must be truly anonymous. If this data is not truly anonymous and is being collected, use, and shared in a widespread manner, this situation would run contrary to

⁶¹¹ *SK HIPA*, *supra* note 544, s 3(2)(a):

This Act does not apply to: (a) statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified.

⁶¹² *MB PHIA*, *supra* note 545, s 3:

This Act does not apply to statistical health information, or to health information that does not, either by itself or when combined with other information available to the holder, allow an individual to be readily identified.

⁶¹³ *NB PHIPAA*, *supra* note 546, s 3(2)(a):

Unless otherwise specifically provided in this Act, this Act does not apply to (a) anonymous or statistical information that does not, either by itself or when combined with other information available to the holder of the information, permit individuals to be identified.

⁶¹⁴ *NS PHIA*, *supra* note 548, s 5(2)(a):

This Act does not apply to...

(a) statistical, aggregate or de-identified health information.

⁶¹⁵ *PEI HIA*, *supra* note 549, s 4(1)(a):

Unless otherwise specifically provided in this Act, this Act does not apply to

(a) anonymous or statistical information that does not, either by itself or when combined with other information available to the holder of the information, permit individuals to be identified.

the individual's fundamental right to control his or her personal health information.⁶¹⁶ However, recall from the discussion of data exclusivity at section 3.3.1, above, that clinical trial data in Canada can never be de-identified because the federal government does not allow it.

Research has shown that individuals can be re-identified from information that was presumed to be anonymous.⁶¹⁷ In their re-identification study, Latanya Sweeney et al used 1,130 public profiles of individuals who shared their genetic data for the Personal Genome Project (PGP), which was launched in 2006 in order to sequence the information and make it publicly available in order for researchers to gain further insight into genetic disease mechanisms and for individuals to learn about their own genetic profiles for disease risk.⁶¹⁸ Roughly half of the PGP profiles consisted of an individual's date of birth, gender, and 5-digit postal code, and Sweeney et al used a voter registration list and a public records website to re-identify the PGP data according to individual names. The researchers ultimately produced a list of 241 unique names for 42% of profiles in the entire PGP dataset, and PGP staff confirmed that 84% of the matches were correct.⁶¹⁹ In addition to DNA information, many participants revealed sensitive conditions including abortions, sexual abuse, illegal drug use, and clinical depression.⁶²⁰

⁶¹⁶ Recall, from Chapter Two, the words of LaForest J. in *McInerney*, *supra* note 375 at para 22 with respect to the expectation regarding a patient's continuing interest and control in personal information confided to a physician.

⁶¹⁷ This research, and most research on re-identification, was conducted using publicly available data sets. Nevertheless, this research is still relevant in light of the fact that some Canadian personal health information protection statutes authorize a technique called data matching, which is done without individuals' consent. For example, data matching under Alberta's *Health Information Act, AB HIA*, *supra* note 542, s 1(1)(g), involves the creation of identifying information through the combination of non-identifying or identifying information or "other information" from two or more electronic databases "without the consent of the individuals who are the subjects of the information."

⁶¹⁸ Sweeney et al, *supra* note 403 at 2.

⁶¹⁹ *Ibid* at 3. The percentage of correctly matched profiles and names was as high as 97% if the use of possible nicknames was considered.

⁶²⁰ *Ibid* at 3-4.

Importantly, the PGP dataset consisted of data from individuals who had expressly consented to the public sharing of their DNA information and who also had control over the extent of the information that they wished to disclose. However, as will be discussed in section 3.4.4 of this thesis, some personal health information protection statutes authorize the creation of individually identifying information through data matching, which can occur without the consent of the individual,⁶²¹ albeit with the approval of the requisite research ethics boards.

The ability to create identifying information from the availability of multiple data sets raises the possibility of negative consequences for individuals, especially with respect to genetic discrimination. For example, insurers routinely rely on an individual's family history and health status when determining risk classifications for health or life insurance policies that are sensitive to mortality risks.⁶²² Although predictive genetic information may be necessary for an accurate assessment of risk and the subsequent determination of the terms of insurance coverage,⁶²³ genetic information is nonetheless, at best, "no more than probabilistic regarding the materialization of the risk in question," particularly with respect to conditions with multiple causal factors, and the individual can remain asymptomatic.⁶²⁴ In this way, re-identification of publicly available information by certain parties, such as insurers, can contribute to the denial or limitation of an individual's access to private insurance, thereby affecting his or her ability to respond to unfortunate life events.

⁶²¹ For example, see *AB HIA*, *supra* note 542, s 1(1)(g) and *NS PHIA*, *supra* note 548, s 52(a).

⁶²² Elizabeth Adjin-Tettey, "Potential for Genetic Discrimination in Access to Insurance: Is there a Dark Side to Increased Availability of Genetic Information?" (2013) 50 *Alberta L Rev* 577 at para 20.

⁶²³ *Ibid.*

⁶²⁴ *Ibid* at para 7.

Ultimately, it is the correlation between the individual's name and another piece of information, such as being afflicted by a certain condition or disease that can create the risk of harm to the individual upon disclosure.⁶²⁵ The volume of available data accordingly plays an important role in increasing the likelihood for re-identification because it increases the potential for correlation between variables.⁶²⁶ The more detailed the information in a data set, the easier it is to re-identify an individual in that data set.⁶²⁷ Nevertheless, commentators such as Ann Cavoukian and Daniel Castro have asserted that, although re-identification of data sets is possible, the chance of re-identification is relatively difficult in actual practice, such that the use of proper de-identification tools render re-identification extremely unlikely.⁶²⁸ However, Cavoukian and Castro also acknowledge that removing only direct identifiers – i.e. variables that provide an explicit link to a data subject and that can directly identify an individual – is often insufficient to ensure the de-identification of information.⁶²⁹ The problem of de-identification involves “quasi-identifiers,” which are variables that may not directly identify individuals but are highly correlated with unique identities and may thus be used for indirect re-identification, either alone or in combination with other available information.⁶³⁰ Cavoukian and Castro accordingly recommend that, in creating de-identified datasets,

⁶²⁵ Gratton, *supra* note 406 at 173.

⁶²⁶ *Ibid* at 174.

⁶²⁷ Institute of Medicine, *supra* note 392 at 100.

⁶²⁸ Ann Cavoukian & Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*, Information and Privacy Commissioner of Ontario, (June 16, 2014), available online: < <http://www2.itif.org/2014-big-data-deidentification.pdf>> (accessed August 8, 2017) at 10-11 [Cavoukian & Castro], citing Khaled El Emam et al, “De-Identification Methods for Open Health Data: The Case of the Heritage Health Prize Claims Dataset” (2012) 14 *Journal of Medical Internet Research* 1-29: El Emam et al used a core dataset of 3 years' worth of de-identified demographic and claims data on 113,000 patients and estimated that the probability of re-identifying an individual was 0.0084 (or less than 1 percent of the individuals in the dataset).

⁶²⁹ Cavoukian & Castro, *ibid* at 9.

⁶³⁰ *Ibid*.

organizations should perform initial risk assessments and should consider the current techniques regarding de-identification and re-identification.⁶³¹

It is thus a question of achieving a balance between utility and anonymity of information, since “data can be either useful or perfectly anonymous, but never both.”⁶³² The ability to access multiple records and the absence of precise limitations on data collection can accordingly render it easier for analysts to match and re-identify information.⁶³³ Gratton thus proposes that the notion of identifiability should be interpreted in light of the information’s overall sensitivity.⁶³⁴ In addition to the “intimate” nature of the information and the extent of its availability to third parties or the public upon disclosure, Gratton asserts that an analysis of the definition of *personal* information should also consider whether the information collected may create a risk of harm upon use or disclosure, since the risk of harm to an individual is minimal if an organization merely collects personal information without using it and also protects the information against disclosure.⁶³⁵

3.4.4. Contemplating Technological Realities: Personal Health Information Statutes, Data Matching, and Re-Identification of the Individual

Protecting individual privacy is particularly challenging in 2017, where the variety of data, size of data sets, and scope of data analyses are “unprecedented.”⁶³⁶ Even if Canadian law did not require that clinical trial participants remain capable of being identified, de-identifying data does not eliminate all risk of re-identification of data

⁶³¹ *Ibid.*

⁶³² *Ohm, supra* note 605 at 1704.

⁶³³ *Ibid* at 1767.

⁶³⁴ *Gratton, supra* note 406 at 161.

⁶³⁵ *Ibid.*

⁶³⁶ *Ibid* at 146.

subjects, since reducing this risk to zero would destroy or at least significantly impair the utility of the data for subsequent research.⁶³⁷ There is always some level of risk that individual participant data, even de-identified, could be used to re-identify a research participant, especially if “auxiliary information were linked with the clinical trial data set.”⁶³⁸ Using such auxiliary information, it may be possible to infer or learn information about individuals in a research data set, including the presence of sensitive conditions such as alcoholism or mental illness.⁶³⁹

Research Ethics Committees are aware of the need to protect individual privacy interests. For example, the TCPS 2 notes that where data is linked to different sources of publicly available information, such linkages could give rise to new forms of identifiable information, thereby raising issues of privacy and confidentiality.⁶⁴⁰ Accordingly, the TCPS 2 requires that researchers who propose to engage in data linkage must obtain approval from the appropriate Research Ethics Board before carrying out the linkage, unless the research relies exclusively on publicly available information.⁶⁴¹ In addition to requirements to describe the data that will be linked and the likelihood that identifiable information will be created through data linkage, researchers must also prove to the applicable Research Ethics Board that the linkage is essential to the research and that security measures will be implemented to protect the information.⁶⁴² The TCPS 2 requirements reflect the reality that a growing number of databases and the advanced technological capacity to link databases together create new risks to confidentiality of

⁶³⁷ Institute of Medicine, *supra* note 392 at 146.

⁶³⁸ *Ibid* at 55, citing C Dwork, “Differential Privacy: A Cryptographic Approach to Private Data Analysis,” in J Lane et al, eds, *Privacy, Big Data, and the Public Good* (New York: Cambridge University Press, 2014) 296-322.

⁶³⁹ *Ibid.*

⁶⁴⁰ *TCPS 2*, *supra* note 16 at 16.

⁶⁴¹ *Ibid*, art 5.7.

⁶⁴² *Ibid.*

information, in which the linkage of de-identified or anonymized data may permit re-identification of individuals.⁶⁴³ Thus, data linkage is directly relevant to the risk of re-identification.

Most important to this thesis, personal data protection legislation has acknowledged modern technological realities. Certain Canadian personal health information protection statutes have expressly addressed “data matching,” and consequently have, indirectly, addressed the issue of re-identification in doing so. For example, Alberta’s *Health Information Act* defines data matching as meaning:

...the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information.⁶⁴⁴

With respect to health information custodians, Alberta’s *Health Information Act* states that the custodian may perform data matching using information that “is in its custody or under its control”⁶⁴⁵ and may also perform this technique by “combining information that is in its custody or under its control with information that is in the custody or under the control of another custodian.”⁶⁴⁶ Importantly, since data matching occurs without the consent of the individual subject of the information, custodians who engage in data matching under Alberta’s *Health Information Act* are required to conduct a privacy impact assessment before data matching can be performed.⁶⁴⁷ These privacy

⁶⁴³ *Ibid* at 67.

⁶⁴⁴ *AB HIA, supra* note 542, s 1(1)(g). Nova Scotia’s *Personal Health Information Act, supra* note 548, s 52(a) defines “data matching” in an almost identical manner, except the databases do not necessarily have to be electronic (even though, in practice, they almost certainly will be electronic):

“data matching” means the creation of individual identifying health information by combining individual identifying or non-identifying health information or other information from two or more databases without the consent of the individuals who are the subjects of the information.

⁶⁴⁵ *AB HIA, ibid*, s 69.

⁶⁴⁶ *Ibid*, s 70(1).

⁶⁴⁷ *Ibid*, s 70(2).

impact assessments must describe how the information for use in the data matching will be collected and must also delineate the use and disclosure for the information that will be created by the data matching.⁶⁴⁸ The other Canadian jurisdictions that authorize data matching by health information custodians are New Brunswick,⁶⁴⁹ Nova Scotia,⁶⁵⁰ the Northwest Territories,⁶⁵¹ and Prince Edward Island.⁶⁵² In enacting rules to address the technique of data matching, these jurisdictions have acknowledged that the availability of multiple data sets can create identifying information that might have otherwise been unavailable.

Identifying information that is created from data matching will be protected under personal health information protection statutes and other personal data protection legislation across Canada in accordance with statutory definitions of personal health information therein. However, the ability to engage in data matching in the first place emphasizes the importance of clarifying the definition of identifiability with respect to information that has been rendered anonymous.

⁶⁴⁸ *Ibid.*, s 70(3).

⁶⁴⁹ See *NB PHIPAA*, *supra* note 546, ss 56-57. Section 56(1)(c) requires a privacy assessment to be conducted in the event that personal health information is to be used in data matching, and section 56(2) mandates the privacy assessment to “describe...how the proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual to whom the information relates.”

⁶⁵⁰ See *NS PHIA*, *supra* note 548, s 59(3)(j): This provision requires an explanation of why data matching is required for research.

⁶⁵¹ *NT HIA*, *supra* note 551, s 36(2):

Subject to the regulations, a health information custodian may, for a purpose for which personal health information may be used or disclosed under this Act, (a) create or produce personal health information by combining information from two or more electronic databases or records; or (b) compare personal health information about an individual on two or more electronic databases or records.

This legislation thus authorizes data matching but does not contain extensive rules regarding the issue.
⁶⁵² See *PEI HIA*, *supra* note 549, ss 26-32. Section 25(1)(c) requires the custodian to prepare a privacy impact assessment “if a custodian performs data matching with personal health information collected by it or with any personal health information held by another custodian or another person.”

3.4.5. *De-Identification and Re-Identification: Is Data Ever Truly Anonymous?*

Anonymization plays a central role in modern data handling, one in which data handlers try to safeguard the confidentiality of personal information by de-identifying data, including the suppression of patient names.⁶⁵³ However, according to Ohm, legislators must abandon the following notions: 1) the idea that one can single out fields of information that are more “linkable” to individual identity than others; and 2) the idea that individual privacy can be protected when “we do nothing more than identify and remove [personally identifiable information].”⁶⁵⁴ In light of the results of re-identification research, and particularly the fact that personal health information protection statutes expressly acknowledge the ability to combine data together, there is merit in Ohm’s observation that “maybe everything is personally identifiable information to one who has access to the right outside information.”⁶⁵⁵

Some academics note that most measures of the risk of re-identification assume that someone will only attempt to identify a single record in the disclosed database.⁶⁵⁶ Identity disclosure and attribute disclosure are two types of disclosure that are of concern in making raw data on individuals publicly available for secondary research purposes.⁶⁵⁷ Identity disclosure can occur where someone uses indirectly identifying information or “quasi-identifiers”⁶⁵⁸ to assign an identity to a record in a particular data set, whereas

⁶⁵³ *Ohm, supra* note 605 at 1707.

⁶⁵⁴ *Ibid* at 1732.

⁶⁵⁵ *Ibid* at 1723.

⁶⁵⁶ Khaled El Emam et al, “Evaluating the risk of patient re-identification from adverse drug event reports” (2013) 13 BMC Medical Informatics and Decision Making 1-14 at 4.

⁶⁵⁷ *Ibid* at 3.

⁶⁵⁸ *Ibid* at 2. “Direct identifiers” are identifiers that, either by themselves or in combination with other readily available information, can be used to uniquely identify an individual. These identifiers include an individual’s credit card number, health card number, and social insurance number. On the other hand, “quasi identifiers” constitute the background knowledge about an individual in a data set, which can be used either alone or in combination with each other to re-identify a record based on probabilities. Quasi

attribute disclosure can occur when someone discovers a new, sensitive characteristic about a patient in a database without necessarily knowing which specific record belongs to the patient.⁶⁵⁹ Disclosing information that is not associated with an individual's name may create the mistaken belief that the individual is truly anonymous, thereby promoting a false sense of security and increasing the willingness of the individual to share the information publicly.⁶⁶⁰

The willingness to freely disclose de-identified information is also relevant to organizations that are health information custodians. Personal health information protection laws do not apply to de-identified information: for such information, no limitations regarding collection, use, and disclosure of information apply.⁶⁶¹ Rather than focusing on the utility or merits of de-identification, this thesis focuses instead on the question of clarifying what it means to be identifiable in 2017, given the power of current information technology and the assumption still reflected in some personal health information protection statutes that data can still actually be rendered truly anonymous and thus does not merit personal data protection. The evidence is that the assumption of de-identifiability is not valid. Therefore, personal data protection legislation needs to preserve personal data protection for all data regardless of purported status in terms of identifiability or anonymization.

identifiers include demographic information such as an individual's sex, date of birth, ethnic origin, marital status, and total income.

⁶⁵⁹ *Ibid* at 2-3. With respect to attribute disclosure, the authors note that an analyst does not have to know which record belongs to the specific patient. For example, if the data set shows that a patient was given a lab test for creatine kinase, the analyst can infer that the patient showed symptoms of a heart attack.

⁶⁶⁰ Sweeney et al, *supra* note 403 at 1.

⁶⁶¹ For example, please refer to the previous discussion in section 3.4.3 of this thesis, which found that some health-specific personal data protection statutes authorized the collection, use, and disclosure of de-identified data for *any* purpose: see *AB HIA*, *supra* note 542, ss 19, 26 & 32; *NB PHIPAA*, *supra* note 546, ss 30, 33 & 36; *PEI HIA*, *supra* note 549, ss 20, 22(4) & 23(4); *YK HIPMA*, *supra* note 550, s 14; *NT HIA*, *supra* note 551, s 1(4).

3.4.6. Withdrawal of Consent to Use and Disclosure of Personal Information: A Potential Conflict with Data Exclusivity?

Although it appears to be uncommon for patients who withdraw consent to participation in a clinical trial to also request the removal of their previously collected data, such requests do occur.⁶⁶² However, in addition to the fact that the withdrawal of patient data from a clinical trial dataset can reduce the integrity of the sample and compromise the scientific validity and generalizability of the research,⁶⁶³ the *Food and Drug Regulations* oblige clinical trial sponsors to retain, for 25 years, all records involved in a clinical trial,⁶⁶⁴ including those that would enable the individual to be identified.⁶⁶⁵

This mandated requirement to retain all records involved in a clinical trial is directly relevant to the data exclusivity right of pharmaceutical companies with respect to clinical trial data. The requirement, however, appears to conflict with an individual's right to control his or her personal data in terms of the right to withdrawal of the data from a clinical trial dataset. According to the OECD Privacy Guidelines, individuals should have the right to have data "erased" upon successfully challenging data related to them.⁶⁶⁶ To explore this potential conflict between personal data protection and data exclusivity, this thesis analyzed the private sector statutes that govern clinical trial

⁶⁶² Chenglin Ye et al, "Data withdrawal in randomized controlled trials: Defining the problem and proposing solutions" (2011) 32 *Contemporary Clinical Trials* 318 at 319: These Canadian authors note that, in one of their randomized controlled studies, of the 60 of 1102 patients who withdrew consent to participation in a randomized clinical trial, only one patient requested withdrawal of his or her data. The researchers also seem to accept a right of withdrawal under Canadian personal data protection legislation, although they do not provide pinpoint citations within the Canadian legislation they cite.

⁶⁶³ Andre P Gabriel & Charles P Mercado, "Data Retention after a Patient Withdraws Consent in Clinical Trials" (2011) 3 *Open Access J Clin Trials* 15 at 17 [*Gabriel & Mercado*].

⁶⁶⁴ See *Food and Drug Regulations*, *supra* note 5, s C.05.012(4).

⁶⁶⁵ *Ibid*, s C.05.012(3)(d).

⁶⁶⁶ See OECD Guidelines, *supra* note 92, Part Two at para 13.

sponsors in Canada.⁶⁶⁷ Specifically, this thesis examined PIPEDA and the private sector statutes from British Columbia, Alberta, and Quebec, in order to determine whether these statutes authorize a right of absolute withdrawal of personal information that has already been collected.

Of the four statutes analyzed, Quebec's *An Act respecting the Protection of Personal Information in the Private Sector* ("Quebec's Act") is the only statute that has expressly implemented the right to "erase" personal information in the same manner contemplated by the OECD Privacy Guidelines. Quebec's *Act* grants the individual a right of access to personal information held by an "enterprise": upon the individual's request, the enterprise must confirm the existence of the file and communicate any personal information to the individual.⁶⁶⁸ Most important for the purposes of the present discussion, the individual "is entitled to obtain that any personal information collected otherwise than according to law be deleted."⁶⁶⁹ Accordingly, in Quebec, clinical trial participants have express rights of withdrawal of personal data with respect to personal data held by a clinical trial sponsor.

PIPEDA and the private sector statutes from British Columbia and Alberta do not expressly give individuals the right to insist that personal data be erased or deleted by organizations once it has already been collected. Nevertheless, all three of these statutes

⁶⁶⁷ Recall from the discussion in section 3.3.2, above, that clinical trial sponsors that are pharmaceutical companies are not governed by health-specific personal data protection but are governed instead by the applicable private sector statutes in a particular jurisdiction.

⁶⁶⁸ *QC Act*, *supra* note 100, s 27.

⁶⁶⁹ *Ibid*, s 28:

In addition to the rights provided under the first paragraph of article 40 of the Civil Code, the person concerned is entitled to obtain that any personal information collected otherwise than according to law be deleted.

See also *Civil Code*, *supra* note 556, s 40:

Every person may cause information which is contained in a file concerning him and which is inaccurate, incomplete or equivocal to be rectified; he may also cause obsolete information or information not justified by the purpose of the file to be deleted, or deposit his written comments in the file.

require individual consent to the collection, use, and disclosure of personal information.⁶⁷⁰ Furthermore, all of these statutes expressly authorize the withdrawal of individual consent at any time. For example, PIPEDA states that “an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.”⁶⁷¹ British Columbia’s *Personal Information Protection Act* (“British Columbia’s PIPA”)⁶⁷² and Alberta’s *Personal Information Protection Act* (“Alberta’s PIPA”)⁶⁷³ also authorize individuals to withdraw consent to the collection, use, or disclosure of personal information by organizations, such that the organization must cease these activities.⁶⁷⁴

The right to withdraw consent to use and disclosure of personal information has implications in the data exclusivity context. Figure 6 illustrates the reality that clinical trials involve multiple stages with respect to the flow of information, in which the information is ultimately disclosed to Health Canada at the final stage in the course of the regulatory market approval process for new drugs. As discussed earlier, personal health information is first collected by qualified investigators, and this information is subsequently disclosed to the clinical trial sponsor. The information then becomes part of the clinical trial data set which is submitted by the clinical trial sponsor to Health Canada. At each stage, the information is held by a separate organization – and each organization is governed by specific personal data protection legislation – and no single piece of personal data protection legislation governs all of these organizations.

⁶⁷⁰ See *PIPEDA*, *supra* note 101, Sch 1, s 4.3; *BC PIPA*, *supra* note 105, s 6; *AB PIPA*, *supra* note 104, s 7.

⁶⁷¹ *PIPEDA*, *supra* note 101, Sch 1, s 4.3.8.

⁶⁷² *BC PIPA*, *supra* note 105, s 9. The right to withdraw consent is subject to subsections 9(5) and (6), in which, respectively, an individual may not withdraw consent if it would frustrate the performance of a “legal obligation” or if consent had been given to a credit reporting agency.

⁶⁷³ *AB PIPA*, *supra* note 104, s 9. The right to withdraw consent is subject to subsection 9(5), in which the withdrawal of consent does not operate to the extent that it would frustrate the performance of a “legal obligation.”

⁶⁷⁴ See *BC PIPA*, *supra* note 105, s 9(4); *AB PIPA*, *ibid*, s 9(4).

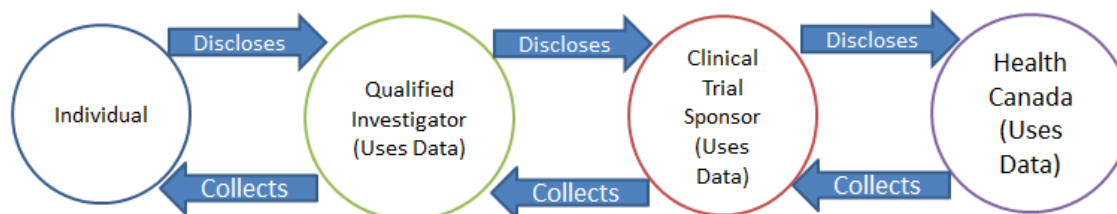


Figure 6 - Flow of Information in a Clinical Trial from a Personal Data Protection Perspective

As demonstrated in Figure 6, the withdrawal of consent to use or disclose personal information at an early stage in the clinical trial (i.e. before the data makes its way from the clinical trial sponsor to Health Canada) will prevent information from moving to the next stage in the chain of information. Thus, although PIPEDA, British Columbia’s PIPA, and Alberta’s PIPA do not grant patients express rights to “erase” data that has already been collected from them in a clinical trial, these statutes nonetheless authorize patients to withdraw consent to the use and disclosure of this information before a clinical trial sponsor can submit it to Health Canada.⁶⁷⁵ Such a withdrawal of consent will essentially “remove” the data from the dataset because the organization that is the custodian will not be able to include the data in the dataset for further study.⁶⁷⁶

⁶⁷⁵ The present discussion focuses on clinical trial sponsors, for whom the data exclusivity right is relevant. If patients were to withdraw consent to the use or disclosure of personal health information held by qualified investigators, the applicable health-specific personal data protection statutes govern the consent to collection, use, and disclosure of personal health information in a particular jurisdiction. See Table 1, above, for the jurisdictions with health-specific personal data protection statutes that would govern qualified investigators therein.

⁶⁷⁶ Disclosure of personal information for “research purposes” constitutes an exception to the requirement that individual consent be obtained by an organization: see *PIPEDA*, *supra* note 101, s 7(c); *BC PIPA*, *supra* note 105, s 21; *AB PIPA*, *supra* note 104, s 20; *QC Act*, *supra* note 100, s 18(8).

Nevertheless, disclosure of personal information for research purposes is often subject to the satisfaction of certain conditions, including the signing of a research agreement: for example, see Alberta’s *Personal Information Protection Act Regulation*, Alta Reg 336/2003, s 14(3), and *BC PIPA*, *supra* note 105, s 21. This thesis does not have any evidence to indicate that clinical trial sponsors have complied with all the requisite conditions for disclosure of personal information for research purposes without individual consent. Further research could establish the following: a) whether these clinical trial sponsors have indeed

Therefore, if patients withdraw consent to use and disclosure of personal information before it is submitted to Health Canada, the clinical trial dataset submitted to the federal government (Health Canada) will not be complete.

3.5. Conclusion

In the past, personal data protection appears not to have even been contemplated as applying to clinical trial data, probably because of the assumption by authors that the data from clinical trials had been anonymized. As such, patients were simply *assumed* to lack rights of control over their data. Current information literature indicates that true anonymization of data is no longer factually possible. As the analyses in this chapter have shown, legislative definitions of personal health information and the record-keeping requirements under the *Food and Drug Regulations* taken together indicate that personal data protection applies to clinical trial data right up to and including the period of data exclusivity protection. This finding represents the first time that a link has been made between the previously diverse legal areas of data exclusivity and personal data protection.

Through an analysis of Canadian data exclusivity and personal data protection legislation, this chapter has demonstrated that data exclusivity does not abrogate the personal data protection rights of the individual clinical trial participant. Instead, personal data protection and data exclusivity regulate different parties' rights of control to the same information. This situation does not necessarily indicate a conflict between the two legislative regimes, although a conflict may arise in the event that a clinical trial

complied with the conditions that would allow them to disclose information for research purposes without individual consent; and b) what this effect would have, from a personal data protection perspective, on the flow of information with respect to the market approval process for new drugs.

participant exercises the right to withdraw consent to the use and disclosure by clinical trial sponsors of personal information under the applicable private sector statutes.

Chapter 4 – Conclusions and Suggestions for Future Research

4.1. Conclusions

Modern intellectual property law seeks to maintain a balance between the rights of individual innovators, the private interests of corporations that dominate intellectual property ownership in many contexts, and the public good in accessing knowledge that will further human progress.⁶⁷⁷ The need for balance among multiple stakeholders involved with intellectual property law is particularly evident in the course of pharmaceutical innovation. As part of this contestation, there is a struggle for control over the confidential information generated in clinical trials.

As discussed in Chapter Two, the protection of commercially-related confidential information, since the mid-nineties, has been classified as intellectual property under international trade agreements including both TRIPS and NAFTA. As described in Chapter Two, Canadian law provides protection both at common law and in civil law consistent with this international trade obligation that such confidential information be protected. In Chapter Two, this thesis noted that the secrecy of confidential information has the potential to endure forever.⁶⁷⁸ The 2012 Supreme Court of Canada decision in *Merck Frosst* reinforces this legal reality: information submitted to the government in innovative drug submissions is exempt from disclosure under the federal *Access Act* (because Parliament accepted the inviolability of commercial confidential information and exempted confidential “third party” information from being accessed by requesters). The decision reinforced the protection of confidential information held by governments from businesses, even when it has been transmitted from the business to the government,

⁶⁷⁷ See Wilkinson, “Marrakesh,” *supra* note 1.

⁶⁷⁸ See Hagen et al, *supra* note 68.

despite the fact that the *Access Act* gives the public a general right to access information in government records.⁶⁷⁹

Both TRIPS and NAFTA also require that nation states confer temporary, exclusive rights, known as “data exclusivity,” upon pharmaceutical companies: rights to the test data that is submitted to regulatory agencies in the course of the market approval process for new drugs. The review of the academic literature on data exclusivity in Chapter Two of this thesis demonstrated disagreements among scholars about the nature and purpose of data exclusivity. This thesis, in Chapter Two, has established that, contrary to the situation of potential permanency established by the law surrounding the secrecy of commercial confidential information in Canada, Canada’s legislated data exclusivity protection actually places a limitation on the period of secrecy in exchange for giving the innovator pharmaceutical company a temporary monopoly on the information. By placing a temporal limit on this secrecy, data exclusivity functions in a manner analogous to classic intellectual property devices such as patent and copyright, which confer limited term monopolies in exchange for public disclosure of information with respect to an invention or work. Accordingly, data exclusivity is consistent with the “bargain” in intellectual property law which seeks a balance between public and private interests. Thus, this thesis demonstrates that a proper understanding of the role of data exclusivity (that it is consistent with, and thus a new species of, intellectual property) runs counter to much of the current literature on data exclusivity which represents data exclusivity as purely a benefit to private interests.⁶⁸⁰

⁶⁷⁹ See *Merck Frosst SCC*, *supra* note 111.

⁶⁸⁰ See sections 2.4.3 and 2.4.4 in Chapter Two.

The need for balance among multiple, potentially divergent interests also raises important questions with respect to an individual's right to control personal information in clinical trials. Since it is individual participants whose personal health information comprises clinical trial data, those individuals have the right to control their personal information in accordance with Canadian personal data legislation⁶⁸¹ and in light of Canada's commitment to the OECD Privacy Guidelines.⁶⁸²

This thesis examined three constructs: 1) the legislative regulation of clinical trials; 2) the data exclusivity right of pharmaceutical companies; and 3) the individual's right to personal data protection. Examination of these three constructs was necessary in order to answer the research question guiding this thesis: **does the data exclusivity right of pharmaceutical companies either operate consistently with or abrogate an individual's right to personal data protection in the clinical trial context?**

To answer the question of whether data exclusivity operates consistently with personal data protection, this thesis analyzed the data exclusivity provisions under Canadian legislation and the definitions of personal health information according to both Canadian health-specific personal data protection legislation and other non-specific Canadian personal data protection legislation relevant to the regulation of personal health information.⁶⁸³ In respect of every province and territory in Canada, this research identified the relevant personal data protection legislation that would apply to qualified investigators and clinical trial sponsors (those who are mandated by the federal *Food and*

⁶⁸¹ For example, see *PIPEDA*, *supra* note 101.

⁶⁸² See *OECD Privacy Guidelines*, *supra* note 92.

⁶⁸³ See Table 1 in Chapter Three for jurisdictions that have health-specific personal data protection.

Drug Regulations to keep records that would enable the identification of clinical trial participants).⁶⁸⁴ Based on this methodology, this thesis found the following:

- 1) Clinical trials involve the collection, use, and dissemination of personal health information;⁶⁸⁵
- 2) According to definitions of personal health information in Canadian personal health information protection statutes,⁶⁸⁶ information must be about an identifiable individual in order to constitute personal health information;
- 3) The existence of applicable health-specific personal data protection does not necessarily mean that all clinical trial sponsors will be covered by this legislation, although all qualified investigators will be. Clinical trial sponsors such as pharmaceutical companies were found to not constitute health information custodians under health-specific personal data protection statutes and were found to be governed instead by private sector personal data protection legislation applicable in each respective jurisdiction.⁶⁸⁷
- 4) For jurisdictions that have not enacted health-specific personal data protection, the public sector and private sector legislation of those particular jurisdictions governed qualified investigators and clinical trial sponsors, respectively.⁶⁸⁸
- 5) Personal health information that initially comprises part of a data set from a clinical trial can technically be “de-identified” using various “anonymization”

⁶⁸⁴ See *Food and Drug Regulations*, *supra* note 5, s C.05.012(3)(d).

⁶⁸⁵ For example, see Institute of Medicine, *supra* note 392 at 93.

⁶⁸⁶ See for example, *PHIPA*, *supra* note 384, s 4(1):

“personal health information”, subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form.

⁶⁸⁷ This legislation was *PIPEDA*, *supra* note 101. By virtue of its status as substantially similar to *PIPEDA*, Alberta’s private sector legislation, the *Personal Information Protection Act*, *supra* note 104 governs clinical trial sponsors in the province of Alberta: see Table 3 in Chapter Three.

⁶⁸⁸ For the jurisdictions and statutes in question, see Table 5 in Chapter Three.

techniques. De-identified data is not subject to personal data protection legislation and can thus be freely used and disclosed by its custodian. At first glance, this would seem to include “de-identified health information” from clinical trials, but for two important findings from this study:

- a) Despite having been subjected to anonymization techniques, data can never be truly anonymous in light of the ability of modern information technology to re-identify individuals. This factual finding that data is never truly anonymous has implications for patient health information that has undergone de-identification and might otherwise be assumed to be excluded from the application of personal data protection laws;
- b) Although clinical trial data might be thought to be capable of de-identification through anonymization techniques during the course of a clinical trial, clinical trial participants must always be capable of being individually identified with their data because of the record-keeping requirements made under the federal *Food and Drug Regulations*.

Based on current statutory definitions under the *Food and Drug Regulations* in Canada, clinical trial data must retain the characteristics of identifiability that bring the data within the Canadian statutory definitions of personal information protected by relevant personal data protection legislation.⁶⁸⁹

- 6) The importance of legislated privacy controls in situation where there is an imbalance of power between those gathering information (here, the qualified investigators and clinical trial sponsors) and clinical trial participants (patients)

⁶⁸⁹ As established above in Chapter Three, the *Food and Drug Regulations* mandate clinical trial sponsors to retain records for a period of 25 years, including the records that would enable the identification of individuals.

has recently been highlighted by the Supreme Court of Canada in *Douez* (2017). In *Douez*, the Court established that contract cannot necessarily oust legislated privacy protections, particularly when there is an imbalance of bargaining power between parties.⁶⁹⁰ In light of *Douez*, and despite whatever past understandings of the role and effect of informed consent to participation in a clinical trial might have been, this thesis indicated in Chapter One that henceforth the “price” for treatment of an individual’s medical condition should not be considered to necessarily include the relinquishing of that individual’s statutory rights to control his or her personal information when it becomes part of the clinical trial data sets going forward through the processes mandated by Health Canada.

As this thesis establishes in Chapter Three, a patient in a clinical trial who applies under the relevant personal data protection legislation to get access to his or her data collected as part of the clinical trial data to be submitted by a pharmaceutical company to the government in an innovative drug submission will be entitled to that access. On the other hand, also discussed in Chapter Three, this thesis establishes that private sector statutes, with the exception of Quebec,⁶⁹¹ do not authorize patients to “erase” personal data from a clinical trial dataset. However, the right to withdraw consent to collection, use, and dissemination of personal information, which is authorized by private sector statutes,⁶⁹² essentially “removes” the data from a clinical trial dataset in practice. Therefore, this thesis has found that, while data exclusivity and personal data protection operate consistently with each other in Canadian law and that data exclusivity does not abrogate the personal data protection rights of the individual, there is a potential for

⁶⁹⁰ See *Douez*, *supra* note 25.

⁶⁹¹ See *QC Act*, *supra* note 100.

⁶⁹² See *PIPEDA*, *supra* note 101; *BC PIPA*, *supra* note 105; *AB PIPA*, *supra* note 104.

conflict between the two legislative regimes if individuals withdraw consent to disclosure of data. As established in Chapter Three, since clinical trials involve multiple stages with respect to the flow of information,⁶⁹³ the withdrawal of individual consent to disclosure of personal data at an early stage of a trial effectively prevents the data from making its way to Health Canada. This “removal” of data can diminish the strength of the evidence that supports the safety and efficacy of a new drug.

These findings are new to the literature about Canada’s data exclusivity provisions. Scholars have argued that data exclusivity hinders access to affordable medicines by delaying the market entry of cheaper generic drugs, thereby negatively affecting public health.⁶⁹⁴ Although one Canadian judge has demonstrated agreement with the perspective that data exclusivity postpones the market entry of lower-cost medicines,⁶⁹⁵ this thesis has demonstrated that other Canadian judges and legal commentators have asserted that data exclusivity actually promotes public health by providing incentives to develop new medicines.⁶⁹⁶ Nonetheless, this earlier debate over the effect of data exclusivity on access to affordable medicines appears to have contributed to an absence of scholarly or judicial attention to the interests of the individual clinical trial participants in the data exclusivity discourse. Despite the fact that clinical trial data comprises personal health information protectable under personal data protection legislation across Canada, the need to consider the potential application of personal data protection laws in the context of data

⁶⁹³ See Figure 6, above, in Chapter Three.

⁶⁹⁴ For example, see Lemmens & Telfer, *supra* note 338.

⁶⁹⁵ See *Canadian Generic FC*, *supra* note 430 at para 76: Mandamin J. states that Canada’s data exclusivity framework does not directly contribute to public safety, since it postpones the introduction of lower cost generic drugs.

⁶⁹⁶ See *Canadian Generic FCA*, *supra* note 451 at para 114; Lietzan, “Myths,” *supra* note 285.

exclusivity appears to have been previously neglected by legislators, judges, and academics.

4.2. Future Research

There is currently very little evidence that patients do withdraw consent to their data being used and disclosed in clinical trials (or that withdrawal of consent with respect to these activities is a sufficiently common occurrence that it affects the integrity of datasets submitted to Health Canada). However, this does not mean that such a situation will never occur in the future. Since there is an evident imbalance of power between individual clinical trial participants and clinical trial sponsors, and in light of the fact that the *Douez* decision prioritizes statutory protections over contractual restrictions in the event of an imbalance of power between parties, there is an urgent need for a solution to the potential conflict between the rights of individuals to control their personal data and the data exclusivity rights of clinical trial sponsors.⁶⁹⁷

Moreover, reconciling this potential conflict depends on legally binding solutions. This thesis focused solely on legally binding instruments with respect to the regulation of clinical trials. This methodological decision revealed potential interpretive issues with the law regarding data exclusivity and personal data protection. While ethical guidelines, as described in Chapter One, that are contained within policies such as the TCPS 2 are informative regarding acceptable practices in clinical research, it is the law, not ethics,

⁶⁹⁷ For example, the private sector statutes of British Columbia and Alberta both state that individuals may not withdraw consent to the collection, use, and disclosure of personal information if this withdrawal would frustrate the performance of a “legal obligation”: see *BC PIPA*, *supra* note 105, s 9(5); *AB PIPA*, *supra* note 104, s 9(5). Since the term “legal obligation” is not defined under these statutes, future research could explore the circumstances that would constitute a “legal obligation” within the meaning of each statute, which would thus clarify the circumstances under which an individual could not stop the flow of data in the context of clinical trials.

that ultimately governs personal data protection and data exclusivity in Canada. Thus, the challenges of the role of personal data protection, in light of data exclusivity, must be considered and addressed by the respective levels of government.

Legally binding solutions would also avoid conflicts with Canada's trade obligations. Article 39(3) of TRIPS does not expressly allow any exceptions for member states to meet the personal data protection rights of individuals.⁶⁹⁸ Similarly, there is no exception under NAFTA to allow for domestic personal data protection obligations. Canada's refusal to enforce its domestic data exclusivity laws on the basis of a conflict with personal data protection could be interpreted as a contravention of Canada's data exclusivity obligations under TRIPS and NAFTA. Member states that fail to enforce intellectual property rights under TRIPS and NAFTA are subject to potential economic sanctions under each agreement. As mentioned previously in Chapter One, TRIPS facilitates a dispute mechanism that authorizes the suspension of "concessions" or "other obligations" in various economic sectors.⁶⁹⁹ NAFTA provides for sanctions in a similar manner, in which Article 2019 of NAFTA directly authorizes the "suspension of benefits" for "measures" that do not conform to NAFTA.⁷⁰⁰ As in TRIPS, complainant

⁶⁹⁸ Wilkinson, "Confidential Information", *supra* note 49 at 288: Wilkinson notes that the language of Article 39(3) of TRIPS mandates the protection of "undisclosed test or other data, the origination of which involves a considerable effort (i.e. clinical trials)." She also observes that there are permitted exceptions to the obligation to protect test data (such as "where necessary to protect the public" or "where steps are taken to ensure that the data are protected against unfair commercial use"). However, Wilkinson ultimately concludes that "there is no permitted exception under TRIPS for meeting the personal data control rights of individual patients in such trials."

⁶⁹⁹ Please refer to section 1.2 of this thesis, which described this sanctions mechanism. See also *GATT 1994*, *supra* note 56 and *DSU*, *supra* note 57.

⁷⁰⁰ *NAFTA*, *supra* note 51, art 2019(1):

If in its final report a panel has determined that a measure is inconsistent with the obligations of this Agreement or causes nullification or impairment in the sense of Annex 2004 and the Party complained against has not reached agreement with any complaining Party on a mutually satisfactory resolution pursuant to Article 2018(1) within 30 days of receiving the final report, such complaining Party may suspend the application to the

parties under NAFTA are also authorized to apply sanctions in different economic sectors.⁷⁰¹ In light of these far-reaching economic reprisals under TRIPS and NAFTA, Canada's failure to implement data exclusivity in accordance with its obligations would have significant effects on Canada's participation in global trade and would thereby result in negative consequences to Canada's national economic interests.

If personal data protection provisions diminish the value of data exclusivity rights to the point where Canada is found not to have met its trade obligations in this regard, there will be pressure on governments to reconcile these interests to preserve the integrity of data exclusivity. On the other hand, the protection of privacy rights, including those embedded in personal data protection statutes, though not an express part of the *Canadian Charter of Rights and Freedoms*,⁷⁰² is part of Quebec's *Charter of Human Rights and Freedoms*⁷⁰³ and may engender constitutional protection. These topics are worthy subjects for future research.

Party complained against of benefits of equivalent effect until such time as they have reached agreement on a resolution of the dispute.

⁷⁰¹ *Ibid*, art 2019(2):

In considering what benefits to suspend pursuant to paragraph 1: (a) a complaining Party should first seek to suspend benefits in the same sector or sectors as that affected by the measure or other matter that the panel has found to be inconsistent with the obligations of this Agreement or to have caused nullification or impairment in the sense of Annex 2004; and (b) a complaining Party that considers it is not practicable or effective to suspend benefits in the same sector or sectors may suspend benefits in other sectors.

⁷⁰² *Charter*, *supra*, note 357.

⁷⁰³ CQLR c C-12, s 5.

Bibliography

INTERNATIONAL TREATIES

Agreement on Trade-Related Aspects of Intellectual Property Rights, April 15 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, (as amended on 23 January 2017), 1869 UNTS 299, 33 ILM 1197.

Berne Convention for the Protection of Literary and Artistic Works, (1886) 828 UNTS 221, revised, July 14, 1967.

General Agreement on Tariffs and Trade, 1994, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 UNTS 187, 33 ILM 1153 (1994).

North American Free Trade Agreement, 17 December 1992, Can TS 1994 No 2 (entered into force 1 January 1994).

Paris Convention for the Protection of Industrial Property, (1883) 828 UNTS 305, revised, July 14, 1967.

World Trade Organization, *Declaration on the TRIPS Agreement and Public Health*, WT/MIN(01)/DEC/2 (14 November 2001), online: <https://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_trips_e.htm>.

World Trade Organization, *Implementation of paragraph 6 of the Doha Declaration on the TRIPS Agreement and public health*, WT/L/540 and Corr.1 (1 September 2003), online: <https://www.wto.org/english/tratop_e/trips_e/implem_para6_e.htm>.

INTERNATIONAL INSTRUMENTS

EEC, *Council Directive 65/65/EEC of 26 January 1965 on the approximation of provisions laid down by law, regulation or administrative action relating to proprietary medicinal products*, [1965] OJ 022, P 0369 – 0373, online: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31965L0065:EN:HTML>> (accessed June 24, 2017).

Organization for Economic Cooperation and Development, *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (2013), online: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

LEGISLATION & REGULATIONS

a) Canada: Constitutional

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (UK)*, 1982, c 11.

Charter of Human Rights and Freedoms, CQLR c C-12, s 5.

b) Canada: Federal

Access to Information Act, RSC 1985, c A-1.

Copyright Act, RSC 1985, c C-42.

Food and Drugs Act, RSC, 1985, c F-27.

Food and Drug Regulations, CRC, c 870.

Interpretation Act, RSC, 1985, c I-21.

Patent Act, RSC 1985, c P-4.

Patent Medicines (Notice of Compliance) Regulations, SOR/93-133.

Privacy Act, RSC, 1985, c P-21.

Regulations Amending the Food and Drug Regulations (Data Protection), SOR/2006-241.

c) Canada: Provincial

Access to Information and Protection of Privacy Act, SNWT 1994, c 20.

Act Respecting the Sharing of Certain Health Information, CQLR c P-9.0001.

An Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1.

Civil Code of Quebec, CQLR c CCQ-1991.

E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c 38.

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31.

General Ontario Regulation, O Reg 329/04.

General Regulation, NB Reg 2010-112.

Health Information Act, RSA 2000, c H-5.

Health Information Act, SNWT 2014, c 2.

Health Information Act, RSPEI 1988, c H-1.41.

Health Information General Regulation, YOIC 2016/159.

Health Information Protection Act, SS 1999, c H-0.021.

Health Information Protection Regulations, RRS c H-0.021 Reg 1.

Health Information Privacy and Management Act, SY 2013, c 16.

Health Information Regulation, Alta Reg 70/2001.

Health Information Regulations, NWT Reg 089-2015.

Medicine Act, 1991, SO 1991, c 30.

Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M 56.

Organizations in the Province of Alberta Exemption Order, SOR/2004-219.

Personal Health Information Act, CCSM, c P33.5.

Personal Health Information Act, SNL 2008, c P-7.01.

Personal Health Information Act, SNS 2010, c 41.

Personal Health Information Custodians in Nova Scotia Exemption Order, SOR/2016-62.

Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05.

Personal Health Information Protection Act, RSO 2004, c 3.

Personal Health Information Regulations, NLR 38/11.

Personal Health Information Regulations, NS Reg 217/2012.

Personal Information Protection Act, SA 2003, c P-6.5.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSBC 1996, c 373.

Regulated Health Professions Act, 1991, SO 1991, c 18.

JURISPRUDENCE

a) Canada

Air Atonabee Ltd v Canada (Minister of Transport), (1989) 27 FTR 194, 27 CPR (3d) 180 (FCTD).

Astrazeneca Canada Inc v Health Canada, 2005 FC 189, 275 FTR 133.

Bayer Inc v Canada (Attorney General), (1999) 243 NR 170, 89 ACWS (3d) 354, aff'g [1999] 1 FC 553, 83 ACWS (3d) 1028.

Bristol-Myers Squibb Co v Canada (Attorney General), 2005 SCC 26, [2005] 1 SCR 533.

Cadbury Schweppes Inc v FBI Foods Ltd, [1999] 1 SCR 142, 167 DLR (4th) 577.

Canadian Generic Pharmaceutical Assn v Canada (Minister of Health), 2010 FCA 334, [2012] 2 FCR 618, aff'g 2009 FC 725, 348 FTR 29 (Eng).

Canadian National Transportation Ltd v Canada (Attorney General), [1983] 2 SCR 206.

Can Aero v O'Malley, [1974] SCR 592, 1973 CanLII 23.

Douez v Facebook, 2017 SCC 33.

Harvard College v Canada (Commissioner of Patents), 2002 SCC 76, [2002] 4 SCR 45.

HJ Heinz Co of Canada Ltd v Canada (Attorney General), 2006 SCC 13, [2006] SCR 441.

International Corona Resources Ltd v LAC Minerals Ltd, [1989] 2 SCR 574, 61 DLR (4th) 14, aff'g (1987) 62 OR (2d) 1, aff'g (1986) 53 OR 2(d) 737.

Jones v Tsige, 2012 ONCA 32, 108 OR (3d) 241.

McInerney v MacDonald, [1992] 2 SCR 138, 1992 CanLII 57.

Merck Frosst Canada Ltd v Canada (Minister of Health), 2012 SCC 3, [2012] 1 SCR 23, aff'g 2009 FCA 166, 400 NR 1, rev'g 2006 FC 1200, 301 FTR 241, 2006 FC 1201, 158 ACWS (3d) 689, aff'g 2005 FCA 215, [2006] 1 FCR 379, rev'g 2004 FC 959, [2005] 1 FCR 587.

Ontario (Public Safety and Security) v Criminal Lawyers' Association, 2010 SCC 23, [2010] 1 SCR 815.

R v Dymment, [1988] 2 SCR 417, 1988 CanLII 10.

R v Stewart, [1988] 1 SCR 963, 50 DLR (4th) 1, rev'g (1983) 149 DLR (3d) 583, 42 OR (2d) 225.

Smith, Kline & French Laboratories Ltd. v Canada (Attorney General) [1987] 2 FC 359 (Fed CA).

Software Solutions Associates Inc v Depow, (1989) 15 ACWS (3d) 298, 25 CPR (3d) 129.

Wyndowe v Rousseau, 2008 FCA 39, 373 NR 301.

b) United Kingdom

Aas v Benham, [1891] 2 Ch 244 (Eng CA).

Coco v AN Clark (Engineers) Ltd., [1968] FSR 415 (Eng HC).

Exchange Telegraph Co v Gregory & Co., [1896] 1 QB 147.

Nichrotherm Electrical Co v Percy, [1957] RPC 207.

Phipps v Boardman, [1967] 2 AC 46 (UK HL).

Saltman Engineering Co. v. Campbell Engineering Co., (1948) 65 RPC 203 (Eng CA).

Seager v Copydex, [1967] 2 All ER 415 (Eng CA).

GOVERNMENT SOURCES

a) International

Office of the United States Trade Representative, *2003 Special 301 Report*, (May 1, 2003), online: <https://ustr.gov/archive/assets/Document_Library/Reports_Publications/2003/2003_Special_301_Report/asset_upload_file665_6124.pdf>.

Office of the United States Trade Representative, online: <<https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications>> (accessed April 14, 2017).

b) Canadian

Canada Gazette, *Process for the Determination of “Substantially Similar” Provincial Legislation by the Governor in Council*, Part I, (22 September 2001) 135(38), 3618.

Canada Gazette, *Regulatory Impact Analysis Statement*, Part II, (2006) 140(21), 1495.

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, December 2014, online: <http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf>.

Government of Canada, *International Council for Harmonisation (ICH)*, online: <<https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/applications-submissions/guidance-documents/international-conference-harmonisation.html>>.

Government of Canada, *News Release: Government of Canada Proposes Amendments to Intellectual Property Rules for Pharmaceuticals*, (Ottawa: December 13, 2004) online: <<https://www.canada.ca/en/news/archive/2004/12/government-canada-proposes-amendments-intellectual-property-rules-pharmaceuticals.html?=&wbdisable=true>> (accessed April 15, 2017).

Health Canada, *Clinical Trials and Drug Safety*, May 2013, (Accessed April 4, 2017) online: <http://www.hc-sc.gc.ca/hl-vs/alt_formats/pdf/iyh-vsv/med/clinical_trails-essais_cliniques-eng.pdf>.

Health Canada, *Guidance for Records Related to Clinical Trials: Interpretation of section C.05.012 of the Food and Drug Regulations - Division 5*, (May 23, 2006), online: <https://www.canada.ca/content/dam/hc-sc/migration/hc-sc/dhp-mps/alt_formats/hpfb-dgpsa/pdf/compli-conform/gui_68-eng.pdf>.

Health Canada, *Public Release of Clinical Information in Drug Submissions and Medical Device Applications*, (Ottawa: Health Canada, 2017), online: <<https://www.canada.ca/en/health-canada/programs/public-release-clinical-information-drug-submissions-medical-device-applications.html>>.

Legislative Assembly of Prince Edward Island, Office of the Information and Privacy Commissioner, online: <<http://www.assembly.pe.ca/index.php3?number=1013943>> (accessed August 28, 2017).

Patented Medicine Prices Review Board, *Generic Drugs in Canada, 2013* (December 2014) online: <http://www.pmprb-cepmb.gc.ca/CMFiles/NPDUIS/2013-GenReport/PMPRB_NPDUIS_GenericDrugs2013_2014-12_EN.pdf>.

SOURCES ISSUED BY INTERNATIONAL BODIES

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Current and Standing Members* (June 2017), online: <<http://www.ich.org/about/membership.html>> (accessed June 24, 2017).

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice*, Essential Documents for the Conduct of a Clinical Trial, (9 November 2016), available online: <http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6/E6_R2__Step_4.pdf>.

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Mission: Harmonisation for Better Health*, online: <<http://www.ich.org/about/mission.html>> (accessed June 14, 2017).

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Structure and Content of Clinical Study Reports* (30 November 1995), available online: <http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E3/E3_Guideline.pdf>.

Organization for Economic Cooperation and Development, *2013 OECD Privacy Guidelines*, <<https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>> (accessed June 24, 2017).

World Intellectual Property Organization, *Model Provisions on Protection Against Unfair Competition* (1996), online: <[ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_832\(e\).pdf](ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_832(e).pdf)>.

SECONDARY MATERIALS: MONOGRAPHS

Fox, Harold G. *The Canadian Law of Copyright and Industrial Designs*, 2nd ed (Toronto: Carswell Co, 1967).

Gervais, Daniel. *The TRIPS Agreement: Drafting History and Analysis*, 4th ed (London: Sweet & Maxwell/Thomson Reuters, 2012).

- Goodman, Patricia. *Electronic Health Record Regulation in Canada: What the Patient Experience Reveals about the Pursuit of Legislative Harmonization*” (LLM Thesis, University of Western Ontario, 2012) [unpublished].
- Gordon, Michelle Erin. *A Framework for the Protection of Privacy in an Electronic Health Environment* (LLM, University of Toronto, 2010) [unpublished].
- Gurry, Francis. *Breach of Confidence* (Oxford: Clarendon Press, 1984).
- Hagen, Gregory, et al. *Canadian Intellectual Property Law: Cases and Materials*, (Toronto: Emond Montgomery Publications, 2013).
- Institute of Medicine. *Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk* (Washington, DC: The National Academies Press, 2015).
- Perun, Halyna, Orr, Michael & Dimitriadis, Fannie. *Guide to the Ontario Personal Health Information Protection Act* (Toronto: Irwin Law Inc, 2005).

SECONDARY MATERIALS: ARTICLES & CHAPTERS

- Adams, Christopher P & Brantner, Van V. “Estimating the Costs of New Drug Development: Is it Really \$802 Million?” (2006) 25 Health Affairs 420.
- Adjin-Tettey, Elizabeth. “Potential for Genetic Discrimination in Access to Insurance: Is there a Dark Side to Increased Availability of Genetic Information?” (2013) 50 Alberta L Rev 577.
- Andanda, Pamela. “Managing Intellectual Property Rights Over Clinical Trial Data to Promote Access and Benefit Sharing in Public Health” (2013) 44 Max Planck Institute for IP & Competition Law 140.
- Austern, H Thomas. “Drug Regulation and the Public Health” (1964) 39 NYUL Rev 771.
- Baker, Brook K & Geddes, Katrina. “Corporate Power Unbound: Investor-State Arbitration of IP Monopolies on Medicines – *Eli Lilly v. Canada* and the Trans-Pacific Partnership Agreement” (2015) 23 J Intell Prop L 1.
- Barocas, Solon & Nissenbaum, Helen. “Big Data’s End Run around Anonymity and Consent,” in Julia Lane et al, *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014), 44-75.
- Basheer, Shamnad. “The Invention of an Investment Incentive for Pharmaceutical Innovation” (2012) 15 J World Intellectual Prop 305.

- Correa, Carlos M. "Bilateralism in Intellectual Property: Defeating the WTO System for Access to Medicines" (2004) 36 Case W Res J Int'l L 79.
- Correa, Carlos Maria. "Unfair Competition under the TRIPS Agreement: Protection of Data Submitted for the Registration of Pharmaceuticals" (2002) 3 Chic Int'l L 69.
- DiMasi, Joseph A, Hansen, Ronald W & Grabowski, Henry G. "The Price of Innovation: New Estimates of Drug Development Costs" (2003) 22 J Health Economics 151 at 180.
- Dwork, C. "Differential Privacy: A Cryptographic Approach to Private Data Analysis," in J Lane et al, eds, *Privacy, Big Data, and the Public Good* (New York: Cambridge University Press, 2014), 296-322.
- El Emam, Khaled, Rodgers, Sam & Malin, Bradley. "Anonymizing and Sharing Individual Patient Data" (2015) 350 BMJ 1-5.
- El Emam, Khaled et al. "Evaluating the risk of patient re-identification from adverse drug event reports" (2013) 13 BMC Medical Informatics and Decision Making 1-14.
- Evans, Barbara J. "Much Ado about Data Ownership" (2011) 25 Harvard J L& Tech 69.
- Fellmeth, Aaron Xavier. "Secrecy, Monopoly, and Access to Pharmaceuticals in International Trade Law: Protection of Marketing Approval Data under the TRIPS Agreement" (2004) 45 Harvard Int'l L J 443.
- Fried, Charles. "Privacy" (1968) 77 Yale LJ 475.
- Gabriel, Andre P & Mercado, Charles P. "Data Retention after a Patient Withdraws Consent in Clinical Trials" (2011) 3 Open Access J Clin Trials 15.
- Gavison, Ruth. "Privacy and the Limits of Law" (1980) 89 Yale LJ 421.
- Goldman, Dana P et al. "The Benefits From Giving Makers of Small Molecule Drugs Longer Exclusivity over Clinical Trial Data" (2011) 30 Health Affairs 84.
- Gostin, Lawrence O. "Health Information Privacy" (1995) 80 Cornell L Rev 451.
- Gratton, Eloise. "If Personal Information is Privacy's Gatekeeper, Then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information" (2014) 24 Alb LJ Sci & Tech 105.
- Helfer, Laurence R. "Regime Shifting: The TRIPS Agreement and New Dynamics of International Intellectual Property Lawmaking" (2004) 29 Yale J Int'l L 1.

- Henderson, Gail E et al. "Clinical Trials and Medical Care: Defining the Therapeutic Misconception" (2007) 4 PLoS Medicine 1735.
- Hudson, Kathy L & Collins, Francis S. "Sharing and Reporting the Results of Clinical Trials" (2015) 313 JAMA 355.
- Kim, Daria. "Enabling Access to Clinical Trial Data: When is Unfair Use Fair?" (2015) 14 Chi-Kent J Intell Prop 521.
- Lemmens, Trudo & Telfer, Candice. "Access to Information and the Right to Health: The Human Rights Case for Clinical Trials Transparency" (2012) 38 Am J L & Med 63.
- Lietzan, Erika. "A New Framework for Assessing Clinical Trial Data Transparency Initiatives" (2014) 18 Marq Intell Prop L Rev 33.
- Leitzan, Erika. "The Myths of Data Exclusivity" (2016) 20 Lewis & Clark L Rev 91.
- Lexchin, Joel. "The Effect of Generic Competition on the Price of Brand-Name Drugs" (2004) 68 Health Policy 47.
- Mello, Michelle M et al., "Preparing for Responsible Sharing of Clinical Trial Data" (2013) 369 N Eng J Med 1651.
- Moor, James. "The Ethics of Privacy Protection" (1990) 39 Library Trends 69.
- Morgan, Steve et al. "The Cost of Drug Development: A Systematic Review" (2011) 100 Health Policy 4.
- Murphy, Richard S. "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 Geo L J 2381.
- Ng, Emily & Kohler, Jillian Clare. "Finding Flaws: The Limitations of Compulsory Licensing for Improving Access to Medicines – An International Comparison" (2008) 16 Health LJ 143.
- Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701.
- Penk, Alexander J. "Confidential Information in a Commercial Context: An Analysis of "Use" of Confidential Information and the Availability of a Proprietary Remedy for Breach of Confidence" (2000) 9 Auckland U L Rev 470.
- Perry, Mark & Wilkinson, Margaret Ann. "The Creation of University Intellectual Property: Confidential Information, Data Protection, and Research Ethics" (2010) 26 CIPR 93.

- Petrova, Elina. "Innovation in the Pharmaceutical Industry: The Process of Drug Discovery and Development," in M Ding et al, eds, *Innovation and Marketing in the Pharmaceutical Industry: Emerging Practices, Research, and Policies* (New York: Springer, 2014), 19-81.
- Peukert, Alexander. "Individual, multiple and collective ownership of intellectual property rights – which impact on exclusivity?" in *The Structure of Intellectual Property Law: Can One Size Fit All?*, Annette Kur & Vytautas Mizaras, eds, (Cheltenham, UK & Northampton, USA: Edward Elgar Publishing, 2011).
- Rägo, Lembit & Santoso, Budiono. "Drug Regulation: History, Present and Future," in *Drug Benefits and Risks: International Textbook of Clinical Pharmacology*, revised 2nd ed, CJ van Boxtel, B Santoso & IR Edwards, eds, (IOS Press and Uppsala Monitoring Centre, 2008), 65-77.
- Ravvin, Michael. "Incentivizing Access and Innovation for Essential Medicines: A Survey of the Problem and Proposed Solutions" (2008) 1 *Pub Health Ethics* 110.
- Reichman, Jerome H. "Rethinking the Role of Clinical Trial Data in International Intellectual Property Law: The Case for a Public Goods Approach" (2009) 13 *Marq Intell Prop L Rev* 1.
- Solove, Daniel J. "Conceptualizing Privacy" (2002) 90 *California L Rev* 1087.
- Skillington, G Lee & Solovy, Eric M. "The Protection of Test and Other Data Required by Article 39.3 of the TRIPS Agreement" (2003) 24 *Nw J Int'l L & Bus* 1.
- Taubman, Antony. "Unfair Competition and the Financing of Public-Knowledge Goods: The Problem of Test-Data Protection" (2008) 3 *J Intell Prop L* 591.
- Topol, Eric J. "Failing the Public Health – Rofecoxib, Merck, and the FDA" (2004) *New Eng J Med* 351 at 1707.
- Unikel, Robert. "Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets" (1998) 29 *Loyola U Chicago L J* 841.
- Warren, Samuel D & Brandeis, Louis D. "The Right to Privacy," (1890) 4 *Harvard L Rev* 193.
- Weinrib, Arnold S. "Information and Property" (1988) 38 *UTLJ* 117.
- Wilkinson, Margaret Ann. "Battleground between New and Old Orders: Control Conflicts between Copyright and Personal Data Protection," in Ysolde Gendreau, ed, *Emerging Intellectual Property Paradigm – Perspectives from Canada* [Queen Mary Studies in Intellectual Property series edited by Uma Suthersanen], (Cheltenham (UK): Edward Elgar, 2008), 227-266.

- Wilkinson, Margaret Ann. "Confidential Information and Privacy-Related Law in Canada and in International Instruments" in Chios Carmody, ed, *Is Our House in Order? Canada's Implementation of International Law* (Montreal & Kingston: McGill-Queen's University Press, 2010), 275-311.
- Wilkinson, Margaret Ann. "The Confidentiality of Seclusion: Studying Information Flows to Test Intellectual Property Paradigms," in Courtney Doagoo et al (eds), *Intellectual Property for the 21st Century: Interdisciplinary Perspectives on Intellectual Property Law* (Toronto: Irwin Law, 2014), 72-94.
- Wilkinson, Margaret Ann. "What is the role of new technologies in tensions in Intellectual Property?," in Tana Pistorius (ed) *Intellectual Property Perspectives on the Regulation of Technologies* [ATRIP Intellectual Property Law Series] (Cheltenham, UK: Edward Elgar) (in press).
- Yang, Pei-Kan. "Current Developments of Canada's Data Exclusivity Regime: How Does Canada React to NAFTA, TRIPS, and Dangle between Pharmaceutical Innovation and Public Health?" (2009) 4 Asian J WTO & Int'l Health L & Pol'y 65.
- Ye, Chenglin et al. "Data withdrawal in randomized controlled trials: Defining the problem and proposing solutions" (2011) 32 Contemporary Clinical Trials 318.
- Yu, Peter K. "The Political Economy of Data Protection" (2010) 84 Chi-Kent L Rev 777.
- Zimmerman, Gordon J. "Protecting the Value of Intellectual Property: The Basics" (2001) 2001 J Bus Valuation 201.

NON-PEER REVIEWED SOURCES

- Canadian Cancer Trials Group, *Privacy and Confidentiality* (October 1, 2015) at 6-7, online: <<https://www.ctg.queensu.ca/docs/public/policies/PrivacyandConfidentiality.pdf>> (accessed August 6, 2017).
- Canadian Cancer Society, *Why Participate?* online: <<http://www.cancer.ca/en/about-us/our-research/clinical-trials-we-are-funding/?region=on>> (accessed August 6, 2017).
- El Emam, Khaled & Malin, Bradley. *Concepts and Methods for De-Identifying Clinical Trial Data* (2014), Paper commissioned by the Committee on Strategies for Responsible Sharing of Clinical Trial Data <<http://nationalacademies.org/hmd/~media/Files/Report%20Files/2015/SharingData/ElEmamandMalin%20Paper.pdf>>.

Gray, Brian W. *Proposed Changes to Canadian Drug “Linkage” PM(NOC) Regs and Data Exclusivity Provisions*, McCarthy Tétrault (July 28, 2006) <http://www.mccarthy.ca/article_detail.aspx?id=2766>(accessed April 14, 2017).

Sweeney, Latanya, Abu, Akua & Winn, Julia. *Identifying Participants in the Personal Genome Project by Name*, Data Privacy Lab: Harvard University (April 24, 2013), available online: <<https://dataprivacylab.org/projects/pgp/1021-1.pdf>>.

Wilkinson, Margaret Ann. Presentation entitled “What is the Role of New Technology in Tensions in IP?,” at the International Association for the Advancement of Teaching and research in Intellectual Property [ATRIP], Montpellier, Monday July 7, 2014 (opening session), online: <http://law.uwo.ca/about_us/our_people/PDFs/Wilkinson_ATRIP_Montpellier_2014.pdf>.

**Appendix 1: Summary of Major Findings with Respect to Personal Health Information
Protection Legislation**

	AB	SK	MB	ON	NB	NL	NS	PEI	YT	NWT
Definition of personal health info includes identifiability?	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expressly defines de-identification?	No	Yes	No	Yes	Yes	No	Yes	Yes	No	No
De-identified info can be collected, used, disclosed for any purpose?	Yes	No	No	No	Yes	No	No	Yes	Yes	Yes
De-identified info expressly excluded from scope of application?	No	Yes	Yes	No	Yes	No	Yes	Yes	No	No
Data matching (Re-identification) addressed?	Yes	No	No	No	Yes	No	Yes	Yes	No	Yes

Appendix 2: Information Constructs Summary

	Confidential Information	Data Exclusivity	Personal Data Protection
Definition	Information that is intended to be kept secret and is thus communicated only to select parties, if at all.	Allows innovative drug manufacturers to maintain temporary, exclusive rights to information generated in clinical trials.	Provides rules governing processing and handling – i.e. collection, use, and disclosure – of information about an identifiable individual, where this information has made its way into organizations.
Duration of Protection (Canada)	Potentially perpetual	8 years	For the life of the individual; protection after death can vary, ranging from 10 to 30 years. ⁷⁰⁴
Status in Canadian Law	Common law (duty of confidence)	<i>Food and Drug Regulations</i> (federal)	Regulated by federal and provincial statutes Application of a particular statute to personal information depends on whether the organization is a public or private sector organization. Most jurisdictions have also enacted health-specific personal data protection.
Status in International Law	TRIPS, Article 39 (covered as “undisclosed information”) NAFTA, Article 1711	TRIPS: no minimum term of data exclusivity protection; leaves member states free to address term according to their own preferences. NAFTA: requires member states to grant a minimum 5-year protection. Both TRIPS and NAFTA authorize their member states to enact more extensive protection than that required.	OECD Privacy Guidelines

⁷⁰⁴ See Wilkinson, “Control Conflicts,” *supra* note 355 at 255, fn 141.

Appendix 3: List of Acronyms

Acronym	Description
ANDS	Abbreviated New Drug Submission
CSR	Clinical Study Report
DPR	Data Protection Regulation
DSU	Dispute Settlement Understanding
FDA	Food and Drug Administration
ICH	International Council on Harmonization of Technical Requirements for the Registration of Pharmaceuticals for Human Use
ICH-CSR	<i>ICH's Structure and Content of Clinical Study Reports</i>
ICH-GCP	<i>ICH's Guideline for Good Clinical Practice</i>
NAFTA	<i>North American Free Trade Agreement</i>
NDS	New Drug Submission
NOC	Notice of Compliance
PGP	Personal Genome Project
SNDS	Supplemental New Drug Submission
TCPS 2	<i>Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans</i>
TRIPS	<i>Agreement on Trade-Related Aspects of Intellectual Property</i>
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Academic CV

Name: Alison Wong

**Post-secondary
Education and
Degrees:**

University of Western Ontario
London, Ontario, Canada
2016-2017 LLM

University of Western Ontario
London, Ontario, Canada
2013-2016 JD

University of Ottawa
Ottawa, Ontario, Canada
2010-1012 BA

University of Ottawa
Ottawa, Ontario, Canada
2005-2010 BHSc

Academic Awards:

University of Western Ontario, Faculty of Law
J.S.D. Tory Writing Prize
2016

David Thompson Alumni Entrance Scholarship
2013

Social Sciences and Humanities Research Council
Joseph-Armand Bombardier Canada Graduate Scholarship
2012 (declined)

Work Experience:

Graduate Research Assistant
University of Western Ontario
2016-2017

Graduate Teaching Assistant
University of Western Ontario
2016-2017