A FOCUS ON THE RISK OF HARM: APPLYING A RISK-CENTERED PURPOSIVE APPROACH TO THE INTERPRETATION OF “PERSONAL INFORMATION” UNDER CANADIAN PRIVATE SECTOR DATA PROTECTION LAWS

by

Magdalena A. Wojda

B.A., The University of British Columbia, 2004
LL.B., The University of Victoria, 2008

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LAWS

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Law)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

October 2015

© Magdalena A. Wojda, 2015
Abstract

We now live in a world where the Internet is in its second generation, big data is king, and a “Digital Earth” has emerged alongside advancements in 3S technologies, where cyber-attacks and cybercrime are the new trend in criminal activity. The ease with which we can now find, collect, store, transfer, mine and potentially misuse large amounts of personal information is unprecedented. The pressure on data protection regulators continues to mount against this backdrop of frenetic change and increased vulnerability. Law and policy makers around the world tasked with protecting information privacy in the face of these advances are simply struggling to keep pace. One important difficulty they encounter is defining the term “personal information” under data protection laws (DPLs) in order to delineate precisely what type of information enjoys the protection of these legislative instruments. As a result, the meaning and scope of this term have emerged as a pressing issue in scholarly debates in the field of privacy and data protection law. This thesis contributes to these discussions by critically appraising the approaches taken by Canadian courts, privacy commissioners and arbitrators to interpreting the statutory definitions of “personal information” under Canadian private sector DPLs, and showing that a different approach is justified in light of rapidly evolving technologies.

The second part of my thesis recommends a purposive risk of harm focused framework advanced by Canadian privacy scholar Éloïse Gratton as a desirable substitute for existing expansionist approaches to interpreting the definition of “personal information” under Canada’s private sector DPLs. I support my recommendation by discussing the ways in which the proposed risk of harm framework can overcome the shortcomings of existing approaches, and demonstrate this by applying it to previously issued decisions in which Canadian arbitrators and privacy
commissioners or their delegates have applied expansionist approaches to new data types and data gathered by new technologies. In so doing, I demonstrate that the proposed framework better reflects the fundamental purpose of Canadian private sector DPLs: to protect only data that raises a risk of harm to individuals impacted by its collection, use or disclosure.
Preface

This thesis is the original, unpublished, independent work of the author.
# Table of Contents

**Abstract** .......................................................................................................................... ii

**Preface** ............................................................................................................................... iv

**Table of Contents** ................................................................................................................. v

**List of Abbreviations** .......................................................................................................... viii

**Acknowledgements** ............................................................................................................ x

**Dedication** .......................................................................................................................... xi

**Chapter 1: Introduction** ........................................................................................................ 1

1.1 Research Objectives .............................................................................................................. 8

1.2 Scope .................................................................................................................................... 8

1.3 Thesis Structure ....................................................................................................................... 13

**Chapter 2: Key Features and Legislative History of DPLs in Canada** ............................... 15

2.1 Key Features of Canadian DPLs .......................................................................................... 15

2.1.1 Collection of Personal Information .................................................................................. 17

2.1.2 Use and Disclosure of Personal Information ..................................................................... 19

2.1.3 Access, Accuracy, and Correction of Personal Information ............................................ 19

2.1.4 Security and Retention of Personal Information ................................................................. 22

2.1.5 Employee Personal Information ......................................................................................... 23

2.2 Historical Roots and Legislative History of DPLs in Canada ............................................ 24

2.2.1 Development of Conceptions of Privacy ............................................................................ 24

2.2.2 Development of Privacy Protection Legislation in Europe and Canada .............................. 28

2.3 Significance of the Definition of “Personal Information” under Canadian DPLs ............ 38
Chapter 2: Canadian DPLs Aim to Protect Against the Risk of Harm

2.4 Canadian DPLs Aim to Protect Against the Risk of Harm

2.4.1 Purpose Provisions

2.4.2 Subjective and Objective Information-Based Harms

2.4.3 Risk of Harm Principle in Canadian DPLs

Chapter 3: Critique of Existing Interpretations of “Personal Information” under Canadian DPLs

3.1 Expansionist Approaches to Interpreting “Personal Information” in Canada

3.1.1 The Broad Literal Approach under PIPEDA, the Québec Act and Alberta PIPA

3.1.2 The Relative Approach under the BC PIPA

3.2 Critical Appraisal of the Existing Approaches to Interpreting “Personal Information”

3.2.1 Over-inclusiveness and Under-inclusiveness

3.2.2 Uncertainty

3.2.3 Obsolescence

3.2.4 Summary

Chapter 4: Recommending a Purposive Risk of Harm Approach to Interpreting “Personal Information” under Canadian DPLs

4.1 Proposed Approaches to Identifying Information Subject to Data Protection Laws

4.1.1 Abandoning PII

4.1.1.1 Paul Ohm

4.1.1.2 Yuen Yi Chung

4.1.2 Modifying PII

4.1.2.1 Boštjan Berčič & Carlisle George

4.1.2.2 Patrick Lundevall-Unger and Tommy Tranvik
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alberta OIPC</td>
<td>Office of the Information and Privacy Commissioner of Alberta</td>
</tr>
<tr>
<td>BC OIPC</td>
<td>Office of the Information and Privacy Commissioner of BC</td>
</tr>
<tr>
<td>CSA</td>
<td>Canadian Standards Association</td>
</tr>
<tr>
<td>DPI</td>
<td>Deep packet inspection</td>
</tr>
<tr>
<td>DPL</td>
<td>Data protection law</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FIPs</td>
<td>Fair Information Principles</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning Systems</td>
</tr>
<tr>
<td>IP address</td>
<td>Internet Protocol address</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>MDT</td>
<td>Mobile Data Terminal</td>
</tr>
<tr>
<td>OBA</td>
<td>Online behavioural advertising</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OPCC</td>
<td>Office of the Privacy Commissioner of Canada</td>
</tr>
<tr>
<td>PII</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>Québec CAI</td>
<td>Québec’s Commission d’accès à l’information</td>
</tr>
<tr>
<td>SIN</td>
<td>Social insurance number</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDIDs</td>
<td>Unique device identifiers</td>
</tr>
</tbody>
</table>
Legislation

Alberta PIPA  *Personal Information Protection Act*, SA 2003, C P-65

BC PIPA  *Personal Information Protection Act*, SBC 2003, C 63

BC FIPPA  *Freedom of Information and Protection of Privacy Act*, RSBC 1996, C 165

PIPEDA  *Personal Information Protection and Electronic Documents Act*, SC 2000, C 5
Acknowledgements

I offer my sincere gratitude to the faculty, staff, and my fellow students at UBC, who have motivated and assisted me in completing my LL.M. work. I offer particular thanks to Professor Joseph Weiler for graciously agreeing to act as my supervisor; for his encouragement, insight and sense of humour; and for all of his time and effort in this process.

I offer my enduring gratitude to Fran Doyle from Harris LLP for her tremendous support, mentorship, and generosity of spirit over the years. I am deeply grateful for the time, energy and thoughtful input Ms. Doyle contributed to this project as my second reader.

I also owe a sincere debt of gratitude to Professor Michelle LeBaron and Professor Karin Mickelson for their dedicated mentorship and for sharing their wisdom about teaching and learning.

I offer very grateful thanks to Joanne Chung and Associate Dean Ljiljana Biuković, both of whom have been enormously patient, helpful and supportive throughout the program.

Many special thanks also to my co-facilitators and the staff at the UBC Centre for Teaching, Learning and Technology for their inspiring enthusiasm and commitment to excellence in teaching.

Finally, very special thanks are owed to my family, partner, and friends old and new. Their support and encouragement over the years has been overwhelming and humbling.
To Hala
Chapter 1: Introduction

Personal information flows on the information highway like water flowing from streams into rivers, lakes and then oceans. Like water, information comes from a multitude of sources and is used in countless business activities. Once drawn from a source, personal information is mingled with other information streams, and then is processed, modified, sold, used in industrial production, and then allowed to run off, often in an unrecognizable, polluted state.

Individuals, the original source of personal information, do not typically demand that this industrial runoff of information be returned to them. Their concern is that personal attributes and identities are taken and used with wanton abandon, without their knowledge or consent, and exchanged many times to market players without any assurance that the original source is kept accurate and pure. Information, like water, is needed and used by everyone. It must be treated with respect, and subject to reasonable controls enforced by law.¹

In the two decades that have passed since Industry Canada published this description of personal information flows, the increasing pace of technological and societal change has been unrelenting and formidable. We now live in a world where the Internet is in its second generation, big data is king, a “Digital Earth” has emerged alongside advancements in 3S technologies such as Global Positioning Systems (GPS), where cyber-attacks and cybercrime are the new trend in criminal activity. The ease with which we can now find, collect, store, transfer, mine and potentially misuse large amounts of personal information is unprecedented. As David Loukidelis, former Information and Privacy Commissioner of BC, writes, due to the impact of globalization in trade and communications, and the mobility of populations, the “mammoth quantity” of personal information flowing around the world every second of every day “is, alone, cause for wonder.”²

Joseph Alhadeff of Oracle Corporation has described the commercial flows of personal

¹ Ian Lawson, Privacy and the Information Highway, Regulatory Options for Canada (Industry Canada, 1996).
² Michael Power, The Law of Privacy (Markham, ON: LexisNexis Canada Inc., 2013) at vi.
information around the globe as “the new spice routes of trade”. Follow-the-sun workflow accompanied by “vast flows of personal information” through advanced web-based technologies is now the norm in business, and as these vast flows of personal information increase, so does the risk of harm that can result from its misuse. Van den Hoven and Vermaas have described the grave harm that can arise in this context as follows:

Criminals are known to have used databases and the Internet to get information on their victims in order to prepare and stage their crimes. The most important moral problem with “identity theft” for example is the risk of financial and physical damages. One’s bank account may get plundered and one’s credit reports may be irreversible (sic) tainted so as to exclude one from future financial benefits and services. Stalkers and rapists have used the Internet and on-line databases to track down their victims. They could not have done what they did without tapping into these resources.

In an information society there is a new vulnerability to information-based harm. The prevention of information-based harm provides government with the strongest possible justification for limiting the freedom of individual citizens to find out about each other. No other moral principle than John Stuart Mill’s harm principle is needed to justify limitations of the freedom of persons who cause, threaten to cause, or are likely to cause, information-based harms to people. Protecting personal information, instead of leaving it in the open, diminishes the likelihood that people will come to harm, analogous to the way in which restricting the access to fire arms diminishes the likelihood that people will get shot in the street. We know that if we do not establish a legal regime that somehow constrains citizens’ access to weapons, the likelihood that innocent people will get shot increases. In information societies, personal information is comparable to guns and ammunition. We should act accordingly.

Simply put, our information technology is evolving at a dizzying pace and our vulnerability to information-based harm grows along with it.

The pressure on data protection regulators continues to mount against this backdrop of frenetic change and increased vulnerability. The emergence of new data types, new data collection techniques and data mining tools, coupled with the remarkable increase in the volume of data in

3 Ibid. at vi.
4 Ibid. at vi.
circulation and storage, make it easy to link information to specific individuals. Law and policy makers around the world tasked with protecting information privacy in the face of technological and societal advances are simply struggling to keep pace. One important difficulty they encounter is defining the term “personal information” under data protection laws (DPLs), which aim to protect individuals against the information-based harms that can arise from the misuse of their personal information. These harms include subjective harm such as humiliation and embarrassment as well as objective harm such as financial harm and even physical harm, as described above by van den Hoven and Vermaas. The definition of “personal information” is significant in the application of data protection legislation because only information that qualifies as “personal information” triggers the rights and obligations prescribed therein. As a result, the meaning and scope of the concept of “personal information” have emerged as a pressing issue in scholarly debates in the field of privacy and data protection law. Pointing to the inadequacies of existing legal definitions of this term and attempting to overcome these shortcomings, numerous scholars advance new approaches to identifying precisely what information is or should be subject to data protection legislation.

This thesis contributes to the discussion on the meaning of “personal information” by critically appraising the approaches taken by Canadian courts, privacy commissioners, and arbitrators to interpreting the statutory definitions of this term under Canadian private sector DPLs and arguing in favour of a new purposive risk of harm-based interpretive approach that will better

---

6 Éloïse Gratton, Understanding Personal Information: Managing Privacy Risks (Markham, ON: LexisNexis Canada Inc., 2013) at 21.

align with the principal goal these laws seek to achieve. A largely uncontested point that I demonstrate in the chapter that follows is that the fundamental purpose of Canada’s DPLs is to protect individuals against the potential information-based harms that can arise from the improper collection, use, and disclosure of their “personal information”. Canadian DPLs define the term “personal information” as either “information about an identifiable individual” or as a variation of this definition that also centers on the concept of “identifiability”. What is contested in the literature and Canadian case law is how legislators and decision-makers ought to approach the interpretation of this term so as to delineate precisely what types of information fall within the scope of these laws. As I will explain in further detail in the body of this thesis, decision-makers interpreting the statutory definition of “personal information” under private sector DPLs in Canada have adopted “expansionist” approaches based on the concept of identifiability. In essence, under an expansionist interpretive approach, information qualifies as “personal” if it has been linked to a particular person, or might be so linked in the future either directly or in combination with other information. Expansionist interpretive approaches in this context can be contrasted with “reductionist” approaches, under which the tendency is to consider only personal data that has already been specifically associated with a specific person to be “personal information”.

Over time, particularly in the face of rapidly evolving technologies, expansionist interpretations increasingly suffer from a number of woeful inadequacies due to their inflexibility and focus on “identifiability”. Specifically, these interpretations give rise to under- and over-inclusiveness, uncertainty, and obsolescence, all of which makes these interpretive approaches progressively unworkable. Notably, new data types such as Internet Protocol (IP) addresses and cookies, new
practices such as online profiling, and new technologies such as Global Positioning Systems (GPS) amplify the issues of under-inclusiveness and the impending obsolescence of the notion of identity in the context of DPLs. For example, IP addresses, cookies and GPS enable data subjects to be targeted or singled out through unique identifiers even if their real name or date of birth cannot be ascertained. Using these devices, organizations can build “anonymous” profiles and track the online behaviour of these profiles in order to make decisions about them. For example, “an insurance company could refuse to provide health coverage (or to answer questions from a web visitor pertaining to the insurer’s health coverage services) to an individual visiting its website for the main reason that the profile information suggests that this individual has viewed websites for individuals afflicted with certain diseases, even if the insurance company does not have the identity of the individual, and regardless of whether its assumption is in fact accurate.”

Even though the profile information in this example is being use to inflict the type of harm DPLs were designed to prevent, such information would not likely, under an expansionist approach, qualify as personal information attracting the protection of these laws since the insurance company was not in a position to determine the identity of the individual behind the profile.

In addition, in focusing on “identifiability”, expansionist approaches are outmoded in their perception of de-identification and are characterized by the “myth of anonymization”. Paul Ohm has famously written that by collecting ostensibly de-identified pieces of information and connecting them to additional information available to them, adversaries are able to

---

8 Gratton, supra note 6 at 139-140 [citations omitted].
incrementally create a “database of ruin”\textsuperscript{10}, “chewing away bit by byte on individuals’ privacy until their profiles are completely revealed.”\textsuperscript{11} As explained in Section 3.2.3, numerous studies illustrate this point. For example, in a case study conducted in 1999, Latanya Sweeney demonstrated that 87\% of the US population could be identified by matching three innocuous data items: zip code, birthdate, and gender; doing so provocatively, by revealing the health records of the Massachusetts governor at the time.\textsuperscript{12} Expansionist interpretive approaches are falling short in the face of such realities because they are fettered by inflexibility and the concept of “identifiability”.

In the pages that follow, I expand on the inadequacies of the existing expansionist approaches taken under Canadian DPLs and argue that they impede the attainment of the purpose of these laws to facilitate the free flow of information while protecting against information-based harm, as characterized above. In my critique, I build upon the work of European and Canadian privacy scholar, Éloïse Gratton, who advances a purposive framework for interpreting the term “personal information” in a way that reflects the fundamental goal of DPLs by enhancing the protection of data that pose a risk of the type of harm against which these laws actually seek to protect, while facilitating the free flow of information that does not pose such a risk. Gratton proposes a purposive risk of harm-based framework that distinguishes between the three data handling activities governed by DPLs (collection, use, and disclosure) and centers on the particular type of harm (subjective or objective) that arises at each stage.

\textsuperscript{11} Tene, \textit{supra} note 9.
\textsuperscript{12} Latanya Sweeney, \textit{Simple Demographics Often Identify People Uniquely}, Working Paper No. 3 (Laboratory for Int’l Data Privacy, 2000).
Under Gratton’s proposed framework, information being collected by an organization should be considered “personal information” only if it might trigger a risk of harm upon being “disclosed” or “used” (the tests applicable to making this determination are those set out in relation to the points of disclosure and use, which follow). To determine whether information being disclosed qualifies as “personal information” under Gratton’s framework, one must consider the extent to which subjective harm (e.g., feeling of humiliation or embarrassment) might arise as a result, based on three criteria: 1) whether the subject of the information is identifiable; 2) whether the information is of an “intimate nature”; and 3) the extent to which the information is “available”. To determine whether information being used qualifies as “personal information” under the proposed framework, one must consider whether objective harm (e.g., discrimination, or financial or physical harm) is likely to arise as a result. If so, the information qualifies as personal information and the information holder must ensure it is accurate and relevant before using it. If the information does not meet these “data quality” and “relevancy” tests, it should not be used by the organization seeking to use it. Under Gratton’s approach, if the information being used does not trigger a risk of objective harm, it does not qualify as “personal information” and can be used without restriction.

As I argue in detail in Section 4.2, because the purposive risk of harm framework proposed by Gratton is a more nuanced, flexible, and context-based approach, it overcomes the shortcomings of the expansionist interpretive approaches used at present under Canadian DPLs. For instance, with respect to harmful consumer profiling, because the objective harm test under the proposed framework focuses on impact, and not on “identifiability”, the profile in question will be protected by the applicable DPL where its use gives rise to a potential negative impact on the
individual behind the profile (e.g., financial harm or discrimination), whether or not the organization using it can ascertain that individual’s “identity”, in the sense of a name and date of birth, for example. Accordingly, I recommend the proposed framework as a preferable alternative to existing expansionist approaches to interpreting the definition of “personal information” under Canada’s DPLs.

1.1 Research Objectives
The initial goal of this thesis is to survey and critique existing approaches to interpreting the definition of “personal information” under Canada’s private sector DPLs in order to show that a different approach is justified in light of their principal purpose, which is to protect only data that poses a risk of harm to individuals impacted by its collection, use or disclosure. Second, I recommend Gratton’s purposive risk of harm framework as a preferable alternative to existing expansionist approaches to interpreting the definition of “personal information” under these statutes. I support my recommendation by discussing the ways in which the proposed approach can overcome the shortcomings of existing approaches, and demonstrate this by applying the framework to previously issued decisions in which Canadian arbitrators and privacy commissioners or their delegates applied expansionist approaches to new data types and data gathered by new technologies.

1.2 Scope
In force in Canada are multiple privacy statutes governing the collection, use, and disclosure of personal information, in both the public and private sectors. In the public sector, at the federal
level, the Privacy Act\textsuperscript{13} protects the privacy rights of Canadian citizens by regulating the federal government’s collection, use, and disclosure of their personal information. In the public sector at the provincial level, every province and territory has privacy legislation governing the collection, use, and disclosure of personal information held by public bodies: for example, the BC Freedom of Information and Protection of Privacy Act\textsuperscript{14} (BC FIPPA).

In the private sector, entities in federally regulated industries such as banking, telecommunications, shipping and aviation are subject to the Personal Information Protection and Electronic Documents Act\textsuperscript{15} (PIPEDA). In the provincial private sector, private entities are in general subject to either the PIPEDA or provincially enacted privacy protection legislation. In some provinces, both apply. PIPEDA relies on the federal government’s trade and commerce power under section 91(2) of the Constitution Act, 1867\textsuperscript{16} to govern all provincially regulated organizations involved in commercial activity, subject to a unique compromise.\textsuperscript{17} Specifically, in order to balance the need for consistent DPLs across the country against the rights of the province and territories to regulate data protection\textsuperscript{18}, PIPEDA operates under a model of “cooperative federalism”\textsuperscript{19} to exempt from its application commercial activities under the jurisdiction of provinces and territories that have in place a DPL that the Governor in Council deems to be “substantially similar” to the protection of personal information provisions of the

\textsuperscript{13} Privacy Act, RSC 1985, C P-21 [Privacy Act].
\textsuperscript{14} Freedom of Information and Protection of Privacy Act, RSBC 1996, C 165 [BC FIPPA].
\textsuperscript{15} Personal Information Protection and Electronic Documents Act, SC 2000, C 5 [PIPEDA].
\textsuperscript{16} Constitution Act, 1867 (UK), 31 Vict, c 3, reprinted in RSC 1985, App II No 5 [Constitution Act, 1867 (UK)].
\textsuperscript{17} Barbara A McIsaac, Rick Shields & Kris Klein, The Law of Privacy in Canada, loose-leaf (consulted on 7 April 2014) (Toronto: Carswell, 2000) at 1-17.
\textsuperscript{18} Ibid.
federal statute. This means that PIPEDA applies to all private sector organizations in Canada involved in commercial activity except those entities regulated by provinces and territories that have passed a DPL that is “substantially similar” to the PIPEDA. To date, substantially similar legislation has been enacted in Québec, Alberta, and BC (where the legislation is not limited to the commercial context), and in matters relating to health care only, in Ontario, New Brunswick, and Newfoundland and Labrador.

In the health care sector, in addition to Ontario, New Brunswick, and Newfoundland and Labrador, a number of other provinces have enacted legislation dealing specifically with the collection, use, and disclosure of personal health information. These are Alberta, Saskatchewan, Manitoba, and Québec, however, the personal health information legislation in these provinces has not been deemed “substantially similar” to the PIPEDA. Like other Canadian data protection laws, personal health information statutes also impose limits on the collection, use, disclosure and disposal of personal health information and give individuals the right to request the correction of personal health information about themselves. Personal health information generally includes information relating to an individual’s health, health care history, payments made for health care and the individual’s assigned health identification number.

_________________________

20 PIPEDA, supra note 15, s 26(2)(b).
21 An Act respecting the Protection of Personal Information in the Private Sector, CQLR C P-391 [Québec Act].
22 Personal Information Protection Act, SA 2003, C P-65 [Alta PIPA].
23 Personal Information Protection Act, SBC 2003, C 63 [BC PIPA].
25 Personal Health Information Privacy and Access Act, SNB 2009, C P-705 [NB PHIPAA].
26 Personal Health Information Act, SNL 2008, C P-701 [NL PHIA].
28 Ibid. at 8-9.
While it is beyond the scope of this thesis to comment in detail on Canada’s public sector and personal health information privacy protection laws, many of their prescriptions on the collection, use, disclosure, and destruction of, and access to, personal information and personal health information are similar to those found in the DPLs dealing with personal information in the private sector.  

In sum, in the private sector, PIPEDA governs the collection, use, and disclosure of personal information in the course of commercial activities by federally regulated enterprises, as well as personal information in the custody or control of entities in provinces and territories that do not have “substantially similar” legislation. Thus, at the provincial and territorial level, PIPEDA applies in Manitoba, Northwest Territories, Nova Scotia, Nunavut, Prince Edward Island, Saskatchewan, and the Yukon Territory, but not in Québec, Alberta, and BC. It also applies in Ontario, New Brunswick, and Newfoundland and Labrador to private entities other than health information custodians. Inter-provincial and international transactions in any province involving personal information in the course of commercial activities are also subject to PIPEDA. This thesis focuses on the definitions of the term “personal information” in these Canadian private sector DPLs, i.e., PIPEDA, the BC Personal Information Protection Act (BC PIPA), the Alberta Personal Information Protection Act (Alberta PIPA), and Québec’s An act respecting

\[\text{Ibid.}\]
\[\text{PIPEDA, supra note 15.}\]
\[\text{BC PIPA, supra note 23.}\]
\[\text{Alta PIPA, supra note 22.}\]
the Protection of Personal Information in the Private Sector \(^{33}\) (the \(\text{Québec Act}\)). Appendix A lists all of these statutes, and sets out the definition of “personal information” found in each. In this thesis, I will refer to all of these statutes collectively as “Canadian DPLs”.

Notably, since 2008, the bodies administering the \(\text{PIPEDA, BC PIPA}\) and \(\text{Alberta PIPA}\), namely, the Office of the Privacy Commissioner of Canada (OPCC); the Office of the Information and Privacy Commissioner of BC (BC OIPC); and the Office of the Information and Privacy Commissioner of Alberta (Alberta OIPC), have committed to working collaboratively under two consecutive Memoranda of Understanding \(^{34}\) in carrying out their mandates to enforce privacy laws in the private sector. In the most recent 2011 Memorandum, the Commissioners have pledged to continue collaborating in the areas of policy, enforcement, public education and compliance. \(^{35}\) The Memorandum reflects their ongoing intention to share the combined resources of their respective Offices, reduce overlap and inefficiencies, and ensure consistency in the oversight of private sector privacy. \(^{36}\) The Memorandum also clarifies how the Commissioners will share information in carrying out their duties. \(^{37}\) Their commitment to this collaborative work is based on, among other things, a recognition that the BC, Alberta and federal statutes provide

\(^{33}\) \(\text{Québec Act, supra note 21.}\)


\(^{35}\) 2011 Memorandum, supra note 34.

\(^{36}\) \textit{Ibid.} at 2-3.

\(^{37}\) \textit{Ibid.} at 7-8.
for consultation and collaboration; and that there are circumstances in which the Commissioners have concurrent or overlapping jurisdiction.\textsuperscript{38} I note this co-operation between the Commissioners as it is contextually relevant to my argument that a new purposive interpretation of “personal information” would be preferable under all of the Canadian DPLs.

1.3 Thesis Structure

In Chapter 2, I trace the development of global conceptions of privacy; the historical development of privacy protection legislation in Europe and Canada; and the legislative history of Canadian DPLs specifically, as well as their foundational concepts. I also outline the key features of Canada’s DPLs, all of which forms a foundation for 1) emphasizing the extensive nature of the obligations DPLs impose on organizations subject to them, 2) underscoring the significance of the definition of “personal information” under Canadian DPLs, and 3) demonstrating that these statutes were enacted to facilitate the free flow of information for business purposes while protecting individuals against the risk of harm that may arise from the improper collection, use and disclosure of their personal information. In Chapter 3, I first review the expansionist approaches currently used to interpret the definition of “personal information” under Canadian DPLs. Second, I conduct a critical appraisal of these approaches in order to form a foundation on which to argue that these interpretations are inadequate in light of the statutes’ objectives, and that a new approach is justified in light of rapidly evolving technologies. In Chapter 4, I conduct a review of the literature discussing the leading proposed approaches for identifying “personal information” under DPLs in Europe, the US and Canada. I then detail the purposive risk of harm framework proposed by Gratton before discussing the ways in which it

\textsuperscript{38} Ibid. at 2.
would overcome the identified shortcomings of Canada’s expansionist approaches. Finally, in order to demonstrate how the proposed framework might achieve this in practice, I apply it to a sample of cases in which existing expansionist approaches were applied to decide whether new data types, or data collected, used or disclosed through new technologies, qualifies as “personal information”.
In this chapter, I trace the development of global conceptions of privacy; the historical development of DPLs in Europe and Canada; and the legislative history of Canadian DPLs specifically, as well as their foundational concepts. I also outline the key features of Canada’s DPLs, all of which forms a foundation for 1) emphasizing the extensive nature of the obligations DPLs impose on organizations subject to them, 2) underscoring the significance of the definition of “personal information” under Canadian DPLs, and 3) demonstrating that these statutes were enacted mainly to protect individuals against the risk of harm that may arise from the improper collection, use and disclosure of their personal information.

2.1 Key Features of Canadian DPLs

Canadian DPLs regulate the collection, use, and disclosure of personal information. The federal, BC, and Alberta DPLs broadly define “personal information” as “information about an identifiable individual”. In the legislation in Québec, personal information is defined as “information which relates to a natural person and allows that person to be identified”\(^{39}\). Evidently, the key concept in these definitions is “identifiability”. The definition of “personal information” includes employee personal information\(^{40}\) in both Alberta and BC. The \textit{BC PIPA} expressly excludes “contact information”\(^{41}\), and “work product information”\(^{42}\) in BC. The

\(^{39}\) \textit{Québec Act}, supra note 21, s 2.

\(^{40}\) “Employee personal information” is defined in the \textit{BC PIPA}, s 1 as “personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual’s employment”. A similar definition of personal employee information is found in the Alberta \textit{PIPA}.

\(^{41}\) “Contact information” is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.
"Alberta PIPA" excludes from its scope “business contact information” if the collection, use or disclosure is for the purposes of enabling the individual to be contacted in relation to the individual’s business responsibilities and for no other purpose.43

Underpinning Canadian DPLs is a requirement of “reasonableness”, meaning they mandate that organizations collect, use and disclose personal information for “reasonable” purposes only. For example, section 4(1) of the BC PIPA endorses the “reasonable person” test: in discharging its obligations under the Act, “an organization must consider what a reasonable person would consider appropriate in the circumstances.”44 This necessarily limits the information organizations can collect to that which is reasonably necessary to fulfil the stated purpose. Further, organizations subject to DPLs are responsible for personal information under their control even if such information is not in their custody.45 In addition to these general rules, below I briefly review the key features of Canadian DPLs, which relate to the following data handling practices: collection, use and disclosure; access, accuracy, and correction; and security and retention.

42 "Work product information" is defined as information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the personal information.

43 "Alta PIPA, supra note 22, s 4(1)(d)."

44 "BC PIPA, supra note 23, s 4(1)."

45 For example, see BC PIPA, s 4(2).
## 2.1.1 Collection of Personal Information

Under Canadian private sector DPLs, organizations must typically obtain consent from individuals when collecting their personal information.\(^{46}\) Consent is invalid if it is obtained through deception or misrepresentation,\(^{47}\) and once obtained, consent does not authorize use of the personal information for a different purpose.\(^{48}\) In addition, an organization must not make the supply of products or services conditional upon an individual providing consent to the collection of his or her personal information beyond what is necessary to provide the product or service.\(^{49}\)

Consent can be express or implicit, however, what constitutes valid consent varies by jurisdiction. The federal and Québec statues are to a large extent silent on the subject of implied consent. By contrast, the legislation in Alberta and BC expressly sets out certain circumstances in which consent will be implied, including:

- Where personal information is furnished voluntarily and the purpose for the collection, use, or disclosure would be acceptable to a reasonable person;\(^{50}\)
- Where a) the organization gives the individual notice of its intention to collect, use or disclose his/her personal information, and a reasonable opportunity to decline with a reasonable time; b) the individual does not decline; and c) the “collection, use and disclosure is reasonable having regard to the sensitivity of the personal information in the circumstances”.\(^{51}\)

---

\(^{46}\) *PIPEDA, supra* note 15, Sch 1, Cl 4.3; *Alta PIPA, supra* note 22, s 7; *BC PIPA, supra* note 23, s 6; *Québec Act, supra* note 21, s 13; *Civil Code of Quebec*, 1991, C 64 [CCQ], s 37.

\(^{47}\) *PIPEDA, supra* note 15, Sch 1, Cl 4.3.3; *Alta PIPA, supra* note 22, s 10; *BC PIPA, supra* note 23, s 7(3); *Québec Act, supra* note 21, s 14.

\(^{48}\) *PIPEDA, supra* note 15, Sch 1, Cl 4.3.1; *BC PIPA, supra* note 23, s 8(4); *Alta PIPA, supra* note 22, s 8(4); *Québec Act, supra* note 21, s 9.

\(^{49}\) *PIPEDA, supra* note 15, Sch 1, Cl 4.3.3; *Alta PIPA, supra* note 22, s 7(2); *BC PIPA, supra* note 23, s 7(2); *Québec Act, supra* note 21, s 9.

\(^{50}\) *Alta PIPA, supra* note 22, s 8; *BC PIPA, supra* note 23, s 8.

\(^{51}\) *Alta PIPA, supra* note 22, s 8(3); *BC PIPA, supra* note 23, s 8(3).
Canadian DPLs also carve out a number of exceptions under which an organization may collect personal information without consent or from a source other than the individual. These exceptions include:

- Where collection is clearly in the interests of the individual and consent cannot be obtained in a timely way\(^{52}\);
- Where collection is necessary for medical treatment and the individual is unable to give consent\(^{53}\);
- Where it is reasonable to expect that collection with consent would compromise the availability or accuracy of the personal information, and the collection is reasonable for an investigation or proceeding\(^{54}\);
- Where collection is required or authorized by law.\(^{55}\)

Importantly, consent must be informed consent, that is, the organization must explain the purposes for which it will use the information.\(^{56}\) Under the PIPEDA, Alberta PIPA and BC PIPA, consent may be withdrawn at any time, as a result of which the organization must cease collecting, using or disclosing the information in question.\(^{57}\) The Québec Act is silent on the issue of withdrawal of consent.\(^{58}\)

---

\(^{52}\) PIPEDA, supra note 15, s 7(1)(a) BC PIPA, supra note 23, s 12(1)(a); Alta PIPA, supra note 22, s 14(a); Québec Act, supra note 21, s 6.

\(^{53}\) BC PIPA, supra note 23, s 12(1)(b).

\(^{54}\) Ibid., s 12(1)(c); PIPEDA, supra note 15, s 7(1)(b).

\(^{55}\) PIPEDA, supra note 15, s 7 (1)(e); BC PIPA, supra note 23, s 12(1)(b); Alta PIPA, supra note 22, s 14(b).

\(^{56}\) PIPEDA, supra note 15, Sch 1, Cl 4.2; Alta PIPA, supra note 22, s 13(1); BC PIPA, supra note 23, s 10(1); Québec Act, supra note 21, s 8.

\(^{57}\) PIPEDA, supra note 15, Sch 1, Cl 4.3.8; Alta PIPA, supra note 22, s 9; BC PIPA, supra note 23, s 9.

\(^{58}\) Power, supra note 2 at 73.
2.1.2 Use and Disclosure of Personal Information

In the private sector, personal information may be used or shared with third parties only for purposes for which the individual has given consent, or as otherwise permitted under the applicable DPL.\textsuperscript{59} PIPEDA, the Alberta PIPA and BC PIPA require that the purpose be reasonable.\textsuperscript{60} In general, the DPL provisions setting out the requirements for the use and disclosure of information without consent closely parallel the exceptions for collection without consent, as discussed in the preceding section. Examples include where use or disclosure is i) clearly in the interests of the individual, ii) for the purpose of medical treatment, iii) for the purpose of investigations, iv) authorized by law, v) necessary to respond to an emergency that threatens the life, health or security of an individual.\textsuperscript{61} Additional exceptions for sharing personal information without consent include where disclosure is for the purpose of complying with a subpoena, warrant or court order; for law enforcement purposes, for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual; and to a lawyer who is representing the organization.\textsuperscript{62}

2.1.3 Access, Accuracy, and Correction of Personal Information

Private sector DPLs in Canada require organizations to grant individuals access to their personal information, upon request by the individual.\textsuperscript{63} In all jurisdictions except Québec, once an applicant makes an access request, the organization must generally make every reasonable effort

\textsuperscript{59} PIPEDA, supra note 15, Sch 1 Cl 4.3; Alta PIPA, supra note 22, ss 7(1); BC PIPA, supra note 23, ss 14, 15, 17, 18; Québec Act, supra note 21, ss 12, 13.
\textsuperscript{60} PIPEDA, supra note 15, ss 3, 5(3); Alta PIPA, supra note 22, s 16; BC PIPA, supra note 23, ss 14, 17.
\textsuperscript{61} See for example, BC PIPA, supra note 23, s 15(1).
\textsuperscript{62} See for example, Ibid., s 18(1).
\textsuperscript{63} PIPEDA, supra note 15, Sch 1, Cl 4.9; Alta PIPA, supra note 22, s 24(1); BC PIPA, supra note 23, s 23(1); Québec Act, supra note 21, s 27.
to assist the applicant, and to respond without delay, openly, accurately and completely.\textsuperscript{64} The entity must notify the applicant about whether or not it will grant access, and if access is refused, it must provide the reasons for refusal, and inform the applicant of available avenues for review of its decision.\textsuperscript{65} The right of access is, however, subject to a number of discretionary and also mandatory exceptions. Discretionary exceptions to the right of access include where, for example:

- The personal information requested is subject to solicitor client privilege;
- Providing access to the requested information would reveal confidential commercial information which, if disclosed, could reasonably harm the competitive position of the organization;
- The personal information was collected for the purposes of an investigation or legal proceeding;
- The personal information was collected or created by a mediator or arbitrator in the conduct of a proceeding for which he or she was appointed under a collective agreement or enactment, or by a court.\textsuperscript{66}

Mandatory exceptions to the right of access include where it would reveal personal information about another individual; or threaten the health or safety of an individual.\textsuperscript{67} In Alberta and BC, access must also be refused where it would reveal the identity of an individual who has provided personal information about another individual and the individual providing the information does

\textsuperscript{64} PIPEDA, supra note 15, s 8(2); Alta PIPA, supra note 22, s 27(1)(a); BC PIPA, supra note 23, ss 27-29.
\textsuperscript{65} PIPEDA, supra note 15, s 8(7); Alta PIPA, supra note 22, s 29(1)(c); BC PIPA, supra note 23., s 30(1).
\textsuperscript{66} PIPEDA, supra note 15., s 9(3); Alta PIPA, supra note 22., s 24(2); BC PIPA, supra note 23., s 23(3).
\textsuperscript{67} PIPEDA, supra note 15., s 9; Alta PIPA, supra note 22., s 24(3); BC PIPA, supra note 23., s 23(4); Québec Act, supra note 21., s 40.
not consent to the disclosure of his or her identity.\textsuperscript{68} However, if an organization is able to remove the excepted information from the records responsive to the access request, it must do so and provide the redacted document to the applicant.\textsuperscript{69}

In Alberta, organizations must make a reasonable effort to ensure that any personal information collected, used or disclosed by or on behalf of an organization is accurate and complete to the extent that is reasonable for the organization’s purposes in collecting, using or disclosing the information.\textsuperscript{70} Organizations subject to PIPEDA, BC PIPA and Québec’s DPL intending to use personal information to make a decision that directly affects the individual, the entity must make every reasonable effort to ensure that the personal information is accurate and complete.\textsuperscript{71} An applicant who believes there is an error or omission in his or her personal information may request the entity that has the information in its custody or under its control to correct the information.\textsuperscript{72} If an organization makes a determination not to make the correction, the organization must annotate the personal information under its control with the correction that was requested but not made.\textsuperscript{73}

\textsuperscript{68} Alta PIPA, supra note 22, s 24(3)(c); BC PIPA, supra note 23, s 23(4).

\textsuperscript{69} PIPEDA, supra note 15, s 9(1); Alta PIPA, supra note 22, s 24(4); BC PIPA, supra note 23, s 23(5).

\textsuperscript{70} Alta PIPA, supra note 22, s 33.

\textsuperscript{71} PIPEDA, supra note 15, Sch 1, Cl 4.6.1; BC PIPA, supra note 23, s 33; Québec Act, supra note 21, s 11.

\textsuperscript{72} PIPEDA, supra note 15, Sch 1, Cl 4.9.5; Alta PIPA, supra note 22, s 25; BC PIPA, supra note 23, s 24; CCQ, supra note 46, ss 38, 40.

\textsuperscript{73} PIPEDA, supra note 15, Sch 1, Cl 4.9.6; Alta PIPA, supra note 22, s 25(3); BC PIPA, supra note 23, s 24(3); CCQ, supra note 46, ss 38, 40.
2.1.4 Security and Retention of Personal Information

Canadian DPLs require organizations in the private sector to protect personal information in their custody or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. Organizations subject to these statutes are allowed a reasonable or defined retention period. In BC and Alberta, organizations must destroy documents containing personal information, or else remove the means by which the personal information can be associated with identifiable individuals, as soon as it is reasonable to assume that the purpose for which the information was collected is no longer being served by retention, and retention is no longer necessary for legal or business purposes.

Under PIPEDA, retention must be limited to such period as is necessary to fulfill the purposes(s) for initial collection. Under PIPEDA and BC PIPA, if an organization uses an individual’s personal information to make a decision directly affecting the individual, the organization must retain that information for a reasonable period so that the individual has a reasonable opportunity to access it.

Under Québec Act, “[o]nce the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to the time limit prescribed by law or by a retention schedule established by government regulation.”

---

74 PIPEDA, supra note 15, Sch 1 Cl 4.7; Alta PIPA, supra note 22; BC PIPA, supra note 23, s 34; Québec Act, supra note 21, s 10.
75 BC PIPA, supra note 23, s 35(2); Alta PIPA, supra note 22, s 35(2).
76 PIPEDA, supra note 15, Sch 1 Cl 4.5, s 8(8); Power, supra note 2 at 90.
77 PIPEDA, supra note 15, Sch 1 Cl 4.5; BC PIPA, supra note 23, s 35(1).
78 Québec Act, supra note 21, s 12.
2.1.5 Employee Personal Information

The BC PIPA and Alberta PIPA distinguish “employee personal information” from other kinds of “personal information” and the Acts contain specific rules for its collection, use and disclosure without consent. “Personal employee information” under the Alberta PIPA is personal information reasonably required by the organization for the purposes of establishing, managing or terminating an employment or volunteer-work relationship, or managing a post-employment or post-volunteer-work relationship. This definition excludes personal information about the individual that is unrelated to that relationship. “Employee personal information” under the BC PIPA is information about an identifiable employee collected, used or disclosed “solely for the purposes reasonably required to establish, manage or terminate an employment relationship”.

Contact information and work product information are not included in this definition. In addition to the general allowances for collection, use and disclosure without consent, as outlined in the preceding sections, an organization in Alberta or BC may collect, use and disclose employee personal information without consent if the collection is “reasonable for the purposes of establishing, managing or terminating an employment relationship between the employee and the organization”. However, an organization must give prior notice to the employee that it will be collecting, using and disclosing his or her “employee personal information” and explain its purposes for doing so, subject to certain exceptions.

---

79 Alta PIPA, supra note 22, s 1(1)(j).
80 BC PIPA, supra note 23, s 1.
81 Alta PIPA, supra note 22, ss 15(1); 18(1); 21(1); BC PIPA, supra note 23, ss 13(2)(b), 16(2)(b), 19(2)(b).
82 Alta PIPA, supra note 22, ss 15(1); 18(1); 21(1); BC PIPA, supra note 23, ss 13(3)&(4), 16(3)&(4), 19(3)&(4).
2.2 Historical Roots and Legislative History of DPLs in Canada

The purpose underlying Canadian DPLs is central to my critique of existing approaches to the interpretation of “personal information” in Canada and to my argument that a new approach is justified. Determining the purpose for which Canadian DPLs were enacted, as well as understanding the rights and obligations they prescribe, require a review of the history of the development and enactment of these laws. As a result, below I trace the development of global conceptions of privacy; and the historical development of privacy protection legislation in Europe and Canada.

2.2.1 Development of Conceptions of Privacy

A long succession of privacy scholars and experts have recognized that the concept of privacy is “embarrassingly difficult to define”\(^83\), highlighting the “theoretical disarray … plaguing the field.”\(^84\) Privacy is “a highly subjective notion and its interpretation changes over time and space.”\(^85\) Alan Westin has described privacy as “part philosophy, some semantics, and much pure passion.”\(^86\) Nevertheless, or perhaps as a result, elucidating the concept of privacy has been the focus of a vast body of literature. As Barry Sookman observes, the definition of privacy, like other rights and freedoms, depends on the particular interests at stake and has evolved over

---


\(^85\) Barry B Sookman, Computer, Internet and Electronic Commerce Law, loose-leaf (consulted 01 October 2015) ed (Toronto: Thomson Reuters Canada Limited) at 8.2.

\(^86\) Alan Westin, Privacy and Freedom (New York: Athenium, 1967) at x.
time.\textsuperscript{87} In discussing the evolution of DPLs and their definition of the term “personal information”, Éloïse Gratton has identified three waves in theorizing privacy.\textsuperscript{88} The first wave emerged with US Judge Cooley’s definition of privacy as “the right to be let alone”,\textsuperscript{89} a conception that is now generally associated with Warren and Brandeis, who invoked this right in their pivotal article “The Right to Privacy”\textsuperscript{90}. In promoting a distinct privacy tort, Warren and Brandeis espoused a right to be left alone in the face of “recent inventions and business methods” and the threat of new technology in the form of instantaneous photography in the popular press that was “invading the sacred precincts of private and domestic life”.\textsuperscript{91} This formulation of privacy has been followed “to a certain extent over the years”\textsuperscript{92}, but has come under significant academic criticism for being too vague\textsuperscript{93}, overly broad\textsuperscript{94}, or “too limited in today’s context.”\textsuperscript{95} Thus, a better delineated, clearer and more relevant definition was needed.

The second wave in “theorizing privacy” envisaged privacy as “the right to respect for private and family life”.\textsuperscript{96} Rather than being rooted in a fear of technological developments, this conception was born “out of a fear that the carnage of the Second World War would be

\begin{flushleft}
\textsuperscript{87} Sookman, supra note 85 at 8.2.
\textsuperscript{88} Gratton, supra note 6 at 2-6.
\textsuperscript{89} Thomas M Cooley, \textit{A Treatise on the Law of Torts}, 2d ed (Chicago: Callaghan, 1888) at 29.
\textsuperscript{90} Samuel Warren & Louis Brandeis, “The Right to Privacy” (1890) 4:5 Harv Rev 193.
\textsuperscript{91} \textit{Ibid.} at 195; see also Gratton, supra note 6 at page 2.
\textsuperscript{92} Gratton, supra note 6 at 2.
\textsuperscript{93} Hunt, supra note 84 at 179. See also Ruth Gavison, “Privacy and the Limits of Law” (1980) 89:3 Yale LJ 421 at 461, n 120.
\textsuperscript{94} Hunt, supra note 84 at 180-181; Gratton, supra note 6 at 2; See also Gavison, supra note 93 at 438; Anita Allen, \textit{Uneasy Access: Privacy for Women in a Free Society} (Totowa, NJ: Rowman & Littlefield, 1988) at 7.
\textsuperscript{95} Gratton, supra note 6 at 2. See also Daniel J Solove, “Conceptualizing Privacy” (2002) 90:4 Cal Rev 1087 at 1101-1102.
\textsuperscript{96} Gratton, supra note 6 at 2-3.
\end{flushleft}
repeated.” The “right to respect for private and family life” is reflected in the *Universal Declaration of Human Rights*[^98], which states in Article 12 that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation …” This conception of privacy is also reflected in Article 8 of the Council of Europe’s *Convention for the Protection of Human Rights and Fundamental Freedoms*[^99], which states that, subject to certain exceptions, “Everyone has the right to respect for his private and family life, his home and his correspondence”. Gratton writes that this notion of privacy continues to be relevant today and “private life, personal correspondence and communications are often protected by law”.[^100] For example, Articles 36(2) and (6) of the *Civil Code of Québec*[^101], provide that intentionally intercepting or using a person’s private communications, and using a person’s correspondence, manuscripts or other personal documents may be considered invasions of that person’s privacy.

The third wave in theorizing privacy, which conceptualizes privacy as “control over personal information” and underpins current DPLs around the globe, emerged in the late 1960s and early 1970s in response once again to threats associated with advances in technology.[^102] It was the view in Europe during that era that technological developments posed a threat of harm to human dignity and integrity. Examples of specific technological threats about which privacy experts and

[^97]: Ibid. at 3.
[^100]: Gratton, *supra* note 6 at 3.
[^101]: *CCQ*, *supra* note 46, Arts. 36(2) and (6).
[^102]: Gratton, *supra* note 6 at 3-6. For a more detailed discussion on the “control of personal information” conception of privacy and related criticisms, see Hunt, *supra* note 84 at 181-187.
scholars wrote included phone-tapping, electronic eavesdropping, surreptitious observation, hidden television eye-monitoring, truth measurement by polygraphic devices, personality testing for personnel selection, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda.  

As these threats grew, together with the growing use of computers and the development of automated data banks with impersonal methods for collecting data and unprecedented storage capabilities, the European Council sought “adequate protection for the right of personal privacy vis-à-vis these modern scientific and technical methods”. As a result, the conception of privacy transitioned from the right against intrusion on private and family life to a right to control one’s personal information. Westin described privacy in 1967 as “the claim of individuals…to determine for themselves when, how and to what extent information about them is communicated to others”. In 1968, Charles Fried wrote that privacy “is not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves” In a recent article on conceptualizing privacy, Chris Hunt helpfully describes the control conception of privacy as follows:

This theory of privacy is prevalent in the legal and philosophical literature." Westin, an influential early commentator, wrote that privacy is "the claim of individuals . . . to determine for themselves when, how and to what extent information about them is communicated to others"." … Gross and Miller took a similar view and, like Fried, focused on privacy as a state of control one has over the circulation of his personal information rather than as a claim to control. … Conceiving of privacy as a claim to control personal information gets us very close to understanding its essence. Simply put, we intuit privacy as a claim to control, and this intuition is reflected in the social norms that surround us. We feel that this conception of privacy is the reason someone has a moral

103 Gratton, supra note 6 at 4.
104 Ibid. at 5; Van Den Hoven & Vermaas, supra note 5 at 291.
105 Gratton, supra note 6 at 6-13.
106 Westin, supra note 86 at 7.
107 Charles Fried, “Privacy” (1968) 77:3 Yale LJ 475 at 482 [emphasis in original].
claim to keep the contents of his diary secret; and reasonable people reflect that understanding by respecting this right, or at least by intuiting that reading a person's diary violates something we all sense to be private. Furthermore, … the claim to control personal information is closely associated with the values underpinning privacy (especially the values of dignity and autonomy).\(^{108}\)

During the 1960s and 1970s, commentators also began conceptualizing privacy as “the individual’s control over his personal information.”\(^ {109}\) Numerous scholars have since advanced theories of privacy premised on control of information, arguing that this notion of privacy is more relevant today than ever.\(^ {110}\) Gratton writes that we are still currently in this third wave, and that Canadian DPLs have the control conception of privacy as their foundation.\(^ {111}\)

2.2.2 Development of Privacy Protection Legislation in Europe and Canada

Private sector DPLs began to emerge in Europe in the late 1970s and early 1980s based in large part on the control conception of privacy. As states and supra-national bodies began implementing data protection instruments, “their principles converged into a list of universally-recognized data protection standards” which became known as the Fair Information Principles (FIPs).\(^ {112}\) The FIPs provided, and continue to provide, individuals with the means to control the collection, use and disclosure of their personal information by giving them the right to know the information stored about them, the purpose for which their information had been recorded, the particulars of each release of their information, and the right to have inaccurate information

\(^{108}\) Hunt, supra note 84 at 181-182.

\(^{109}\) Gratton, supra note 6 at 9 [emphasis added].


\(^{111}\) Ibid.

\(^{112}\) Gratton, supra note 6 at 6; Report of the BC PIPA Special Committee, supra note 83 at 33.
corrected or erased.\textsuperscript{113} The FIPs, which many still value as premised on the concept of privacy as “control over personal information”, form the foundation for most DPLs currently in force around the globe, including Canadian DPLs.\textsuperscript{114}

It was soon recognized that “uniformity in privacy protection regimes was needed to simplify the rules for business and to facilitate international trade”.\textsuperscript{115} To this end, the Organisation for Economic Co-operation and Development (OECD) implemented its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which articulated the internationally recognized FIPs that had emerged at the time.\textsuperscript{116} The Preface to the OECD Guidelines provides that OECD Member countries considered it necessary to develop Guidelines that would address privacy protection in relation to personal data without interrupting “international flows of data”.\textsuperscript{117} Thus the OECD Guidelines sought to “balance the protection of privacy with the need to ensure that data could continue to flow across borders.”\textsuperscript{118} Canada signed the OECD Guidelines in 1984.\textsuperscript{119}

By the late 1980s, it became clear in Europe that the harmonization of data protection regimes among trading partners had not been successful and this “created problems in the European

\textsuperscript{113} Gratton, \textit{supra} note 6 at 10; Report of the \textit{BC PIPA} Special Committee, \textit{supra} note 83 at 33.
\textsuperscript{114} Gratton, \textit{supra} note 6 at 6.
\textsuperscript{115} Report of the \textit{BC PIPA} Special Committee, \textit{supra} note 83 at 33; Gratton, \textit{supra} note 6 at 14.
\textsuperscript{117} OECD Guidelines, \textit{Ibid.} at Preface.
\textsuperscript{118} McIsaac, Shields & Klein, \textit{supra} note 17 at 1-15.
\textsuperscript{119} \textit{Ibid.}
internal market.” As a result, the European Council adopted the Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EC Directive on Personal Data Protection), which had two primary objectives: 1) to protect the fundamental right to privacy with respect to the handling personal information; and 2) to facilitate the free flow of information across national boundaries. Unlike the OECD Guidelines, the EC Directive on Personal Data Protection is binding on the European Union’s (EU) member states, and requires member nations to restrict external data exchanges to only those jurisdictions that have in place adequate data protection rules. In 2001, the BC Legislative Assembly’s Special Committee on Information Privacy described the Directive as “the most recent and strongest international expression of the fair information principles originally articulated in the OECD Guidelines.”

In Canada during the 1990s, the Canadian Standards Association (CSA) worked together with businesses, consumers and government to develop the 1996 Canadian Standards Association’s Model Code for the Protection of Personal Information. In 2001, the Special Committee on Information Privacy reported that, because the CSA Model Code was developed with input from all economic sectors in Canada, it expresses the FIPs in a manner that reconciles Canadian

---

120 Gratton, supra note 6 at 14.
122 Ibid. at Preamble.
123 Report of the BC PIPA Special Committee, supra note 83. at 14.
124 Ibid. at 33.
business interests with the international standards for data protection. As a result, Canadian commentators view the CSA Model Code as an improvement on the OECD Guidelines. The ten principles articulated in the CSA Model Code are as follows:

1. **Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

2. **Identifying Purposes**: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used.

7. **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

---

126 Report of the *BC PIPA* Special Committee, *supra* note 83 at 34.
127 *Ibid.* at 34.
10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.128

These CSA Model Code principles formed the basis for the substantive provisions of the federal PIPEDA, the enactment of which was motivated by the “the changing international environment with respect to information privacy”129, including the “threat of loss of trade” as a result of the EC Directive on Personal Data Protection.130 McIsaac et al. describe the circumstances leading to the enactment of PIPEDA as follows:

[PIPEDA] represents, at least in part, the federal government’s response to new privacy legislation in Europe. As a result of the European Union’s (EU’s) issuance of the Directive on Data Protection in 1995, the member states of the EU have been obliged to pass data protection laws aimed at the private sector. Since a common feature of these laws is a restriction on the transmission of personal information to jurisdictions outside of the EU that lack comparable privacy safeguards, the Canadian government feared interruptions in data flows between Europe and Canada if counterpart legislation was not put in place. Accordingly, the Act represents Canada’s somewhat grudging move away from a reliance upon industry self-regulation that has hitherto been an explicit facet of federal privacy policy. By initiating these changes, Canada distanced itself from the privacy policy of the United States’ federal government, which has so far resisted calls to adopt comprehensive private sector privacy legislation.131

Against this backdrop, PIPEDA received Royal Assent in April 2000, giving legal effect to the control-based FIPs for the federally regulated private sector by incorporating the principles articulated in the CSA Model Code.132 The ten CSA Model Code principles, as reproduced above, are listed in PIPEDA, Schedule 1, and are incorporated in the Act pursuant to Section

128 CSA Model Code, supra note 125.
129 Report of the BC PIPA Special Committee, supra note 83 at 13.
130 Gratton, supra note 6 at 15. See also Report of the BC PIPA Special Committee, supra note 83 at 14.
131 McIsaac, Shields & Klein, supra note 17.
132 PIPEDA, supra note 15 Sch 1, Cl 5; Report of the BC PIPA Special Committee, supra note 83 at 7; “Complying with the Personal Information Protection and Electronic Documents Act” (17 February 2014), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/fs-fi/02_05_d_16_e.asp> (accessed 12 October 2015).
5. The control-based FIPs were thus wholly adopted into, first, the federal data protection regime, and later into the substantially similar provincial regimes in Canada.

As discussed above, *PIPEDA* regulates data protection in the federal private sector as well as all provincially regulated organizations involved in commercial activity, except those entities regulated by provinces and territories that have passed a DPL that is “substantially similar” to the *PIPEDA*. Provinces with substantially similar legislation are Québec, BC and Alberta. In 1993 Québec became the first Canadian jurisdiction to enact a private-sector data protection law, *An act respecting the protection of personal information in the private sector*. This statute provides “a detailed code of conduct that is currently at the forefront of North American legislation, applying to every business enterprise dealing with personal information in the private sector” in Québec. Québec is considered a pioneer in data protection legislation and the enactment of its private sector DPL was considered by many to be a breakthrough in the area. Similar to the forces underlying the federal government’s motivation to enact *PIPEDA*, the threat of loss of trade arising from the adequate protection requirements of the *EC Directive on Personal Data Protection* was a significant motivating factor underlying Québec’s decision to pass its private sector DPL. The parliamentary debates leading to the enactment of the *Québec Act* repeatedly address the province’s desire to ensure that Québec’s DPL accord with the OECD Guidelines and international data protection efforts, and particularly the measures adopted in

---

133 *PIPEDA*, supra note 15, Sch 1; Cl 5.
134 Gratton, supra note 6 at 15.
135 *Québec Act*, supra note 21.
136 Melsaac, Shields & Klein, supra note 17 at 4.5.1.
138 Gratton, supra note 6 at 15-16; Éloïse Gratton, “Privacy Law in Quebec – Substantially Similar but Different?”, *NYMITY Privacy Interviews with Experts* (November 2012) 1.
Europe. Notwithstanding that it was enacted prior to the *PIPEDA*, Québec’s private sector DPL was deemed “substantially similar” in 2003. However, Québec has challenged the constitutionality of *PIPEDA* (and in particular, its application to federally regulated entities in the province and to provincial entities transferring personal information across the provincial border), in a Québec Court of Appeal case that at the time of writing remains inactive. As it stands, *PIPEDA* continues to apply in the province to federal entities and transborder transfers of personal information.

In 1999, also faced with circumstances “similar to those that brought about the [*PIPEDA*],” the BC government appointed the Special Committee on Information Privacy in the Private Sector, mandating it to examine, inquire into and make recommendations with respect to 1) the protection of personal information in private sector transactions, and 2) the impact of electronic documents on privacy and freedom of information for British Columbians. The Special Committee examined three principal considerations. First, it examined what it described as “the broader context of information privacy” by, for example, reviewing the conception of privacy as “control over personal information”; the emergence of information privacy in the private sector as a public policy issue; the development and substantive content of the OECD Guidelines, the FIPs, the *EC Directive on Personal Data Protection*, and the CSA Model Code; and the development, adoption and principal provisions of the *PIPEDA*, as well as

140 McIsaac, Shields & Klein, *supra* note 17 at 4.5.1.
The rationale for its enactment. The Special Committee concluded that at the time, BC faced circumstances similar to those that prompted the adoption of PIPEDA at the federal level. Second, the Special Committee considered the developments that had given rise to “widespread concern” about the privacy of personal information held in the private sector. Specifically, it examined how the interplay between economic globalization, rapid developments in information technology, and the growth of e-commerce were both impacting the ways in which personal information was collected, used and disclosed, and raising the profile of data sharing practices. The Special Committee stated that these factors had resulted in “an increase in public concern about information privacy in business transactions”. Third, the Special Committee considered the views of businesses and organizations in the private sector, privacy advocates and “interested individuals”. The Special Committee learned that British Columbians were concerned about information privacy and supported its regulation. The business community wanted data protection rules to strengthen the trust of consumers and clients, and because it wanted to operate in a regulatory environment that was consistent for all businesses in all jurisdictions. Consumers wanted their personal information to “be used properly and only by those who [needed] to use it”. Further details on the types of harm about which stakeholders raised concerns are set out below in Section 2.4 in my discussion concerning the fundamental purpose of Canadian DPLs to protect against the risk of information-based harm to the individual.

145 Ibid. at 7.
146 Ibid. at 14.
147 Ibid. at 7.
148 Ibid.
149 Ibid.
150 Ibid.
151 Ibid.
152 Ibid.
153 Ibid.
The Special Committee’s research methodology included attending briefings with BC’s former Information and Privacy Commissioner and other privacy experts, such as representatives of the Information, Science and Technology Agency, and information and privacy scholars. Briefing topics included information technologies and privacy; the meaning of privacy in the private sector context; the status of privacy regulation in other jurisdictions; and health information systems. In addition, the Special Committee consulted with enterprises in the private sector and “interested individuals and organizations” on the issue of information privacy; and also undertook several initiatives to invite public participation, including issuing a call for written submissions and holding public hearings in Victoria, Vancouver and Richmond. Finally, the Special Committee commissioned the Ipsos-Reid Corporation to conduct opinion research among British Columbians to survey their views on information privacy and the need for private sector legislation.

As a result of its inquiry, the Special Committee made four primary findings:

1. Any policy adopted by British Columbia on the matter of information privacy in the private sector had to consider the implications of the PIPEDA for the province;
2. British Columbians “solidly supported” legislation to regulate information privacy in the private sector;
3. British Columbians insisted that any proposed DPL had to balance the private sector’s needs to use personal information against consumers’ rights to information privacy.

---

154 Ibid. at 5.
155 Ibid.
156 Ibid.
(which businesses and individuals agreed was achieved in the FIPs and CSA Model Code); and

4. There was a consensus among individuals, businesses, privacy advocates and legislators that DPLs must be harmonized among all jurisdictions in which private sector organizations do business (i.e., all of the Canadian provinces and territories, and also international trading partners).  

On this basis, the Special Committee made eight recommendations, including that: a) the BC government enact legislation to protect the information privacy of personal information held in the private sector, and that the proposed legislation achieve a fair and workable balance between information privacy and the use of personal information for legitimate private sector purposes; and b) that the proposed legislation harmonize with other Canadian and international jurisdictions, particularly the PIPEDA, by establishing a legal framework based on the FIPs and the CSA Model Code. These two recommendations led to the creation of the BC PIPA, which came into force on January 1, 2004.

Similarly, the Alberta PIPA is the culmination of a consultation process carried out in the fall of 2002, the resulting consultation report issued in January 2003, and associated public

157 Ibid. at 9.
158 Ibid. at 9-10
159 British Columbia, Legislative Assembly, Special Committee to Review the Personal Information Protection Act, Hansard Blues 40th Parl, 2nd Sess, (11 March 2014) [Hansard Blues].
debates.\textsuperscript{161} The Alberta government worked closely with government representatives from BC in order to “harmonize protection rules to ease cross-jurisdictional trade”.\textsuperscript{162} The Alberta PIPA received Royal Assent on December 4, 2003, and came into force on January 1, 2004. It was deemed “substantially similar” to the PIPEDA in October 2004.\textsuperscript{163}

### 2.3 Significance of the Definition of “Personal Information” under Canadian DPLs

As mentioned above, the definition of “personal information” under Canadian DPLs centers on the concept of “identifiability”. For the past 30 or 40 years, the same or very similar definitions have been used repetitively in transnational policy instruments such as the OECD Guidelines and the EC Directive on Personal Data Protection, as well as in domestic DPLs.\textsuperscript{164} The definition is largely consistent throughout Europe and Canada, and “has remained largely unchanged since it was initially articulated in the early 1970s” in Europe.\textsuperscript{165} The functional significance of this definition in the context of a DPL is that it serves as a “jurisdictional trigger” for these statutes.\textsuperscript{166} As also outlined in the preceding sections, Canadian DPLs prescribe numerous rights and obligations relating to the data handling practices of the entities subject to these statutes. Importantly, these rights and obligations are triggered by the determination of whether the information in question qualifies as “personal information” as that term is defined in the applicable DPL. As Gratton states, the “notion of personal information is central to DPLs, as it

\textsuperscript{161} Melsaac, Shields & Klein, \textit{supra} note 17, at 4.4.1.
\textsuperscript{162} \textit{Ibid.}
\textsuperscript{163} \textit{Ibid.}
\textsuperscript{164} Gratton, \textit{supra} note 6, at 18-19.
\textsuperscript{165} \textit{Ibid.} at 19.
\textsuperscript{166} Yuen Yi Chung, “Goodbye PII: Contextual Regulations for Online Behavioral Targeting” (2014) 14 J High Tech L 413 at 415.
defines the object of protection.”167 It is therefore, the “gatekeeper” to privacy protection under these regimes.

With these main features of DPLs in Canada in mind, below I outline the historical development of these statutes and demonstrate that the principal purpose for the enactment of these Acts was to protect individuals against the risk of information-based harm associated with the collection, use and disclosure of their personal information.

2.4 Canadian DPLs Aim to Protect Against the Risk of Harm

In order to form a basis for my critique of the existing approaches to interpreting “personal information” under Canadian DPLs, in this section I demonstrate that the fundamental purpose of these statutes is to protect only data that poses a risk of harm to individuals through its collection, use and disclosure. My discussion includes an overview of the specific types of harm that Canadian DPLs were designed to prevent.

2.4.1 Purpose Provisions

Each Canadian DPL expressly seeks to balance the protection of personal information against the business needs of organizations subject to it.168 This is evident in the purpose provisions set out in each statute. Section 3 of PIPEDA provides:

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

167 Gratton, supra note 6 at 145.
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.

Similarly, Section 2 of the BC PIPA states:

The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect 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.

The language in Section 3 of the Alberta PIPA is virtually identical to the language in the BC and federal statutes:

The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

The Supreme Court of Canada recently stated in Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401\textsuperscript{169} that Alberta PIPA was inspired by the federal PIPEDA, and that the Alberta PIPA’s “stated purpose is almost identical to that of the PIPEDA”.\textsuperscript{170}

Québec enacted its Act respecting the protection of personal information in the private sector\textsuperscript{171} to complete and provide detailed rules of application for Articles 35 to 41 of the Civil Code of Québec\textsuperscript{172}. Article 35 states that “Every person has a right to the respect of his reputation and

\textsuperscript{169} Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62.

\textsuperscript{170} Ibid. at paras 13-14.

\textsuperscript{171} Québec Act, supra note 21.

\textsuperscript{172} CCQ, supra note 46.
privacy.” Articles 35-41, and the private sector DPL enacted under them, embody the Québec government’s “determination to ensure respect for individual reputation and privacy”, based on three “complementary and fundamental principles”. These are i) every person who establishes a file on another person must have a serious and legitimate reason for doing so; ii) the person establishing the file may not deny the individual concerned access to the information contained on the file; and iii) the party establishing the file must also respect certain rules that are applicable to the collection, storage, use and communication of this information.

That Canadian DPLs are seeking to strike a balance between protecting personal information and facilitating commerce is thus not contentious. There is, however, a “heavy weighting here” on the side of protecting personal information. As Perrin et al. have written in discussing the purpose of PIPEDA, the “interests of individuals and the interests of organizations are not in fact balanced in the traditional sense.” This is because, among other things, the interest in the protection of privacy and personal information is characterized as a “right”, while the interests of organizations are characterized in terms of “needs” and “legitimate reasons”.

2.4.2 Subjective and Objective Information-Based Harms

Canadian DPLs aim to protect personal information. More specifically, the danger against which these laws are fundamentally designed to protect is information-based harm. Van den Hoven and Vermaas cogently observe that the “strongest possible justification” for government to impose

---

173 McIsaac, Shields & Klein, supra note 17 at 4.5.1.
175 Perrin et al, supra note 168 at 56.
176 Ibid.
177 Ibid.
DPLs is the prevention of “information-based harm”, that is “harm that is done to persons by making use of personal information about them”, such as financial and physical damage resulting from identity theft, as well as physical harm such as that arising from violent crimes.\(^\text{178}\) Since there is a heightened level of vulnerability to information-based harm in an information society, the prevention of such harm provides government with “the strongest possible justification” for limiting the freedom of individual citizens who “cause, threaten to cause, or are likely to cause, information-based harms to people.”\(^\text{179}\) Van den Hoven and Vermaas cleverly liken personal information in information societies to guns and ammunition, observing that protecting personal information through these types of restrictions “diminishes the likelihood that people will come to harm, analogous to the way in which restricting the access to fire arms diminishes the likelihood that people will get shot in the street.”\(^\text{180}\) It is this kind of harm prevention that lies at the heart of DPLs worldwide, including DPLs in Canada. Specifically, it is the prevention of both subjective and objective information-based harm, as explained below.

Drawing from the work of M. Ryan Calo\(^\text{181}\) and Esther Dyson\(^\text{182}\), Gratton separates the information-based harm against which DPLs aim to protect into two categories: subjective harm and objective harm.\(^\text{183}\) To show that DPLs were designed to target both types of harm, Gratton points to *Council of Europe Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector*, which states:

---


\(^{179}\) *Ibid*.

\(^{180}\) *Ibid*.

\(^{181}\) M Ryan Calo, “The Boundaries of Privacy Harm” 86 Ind LJ 1131.


\(^{183}\) Éloïse 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) 24:1 Albany Law J Sci Technol 105.
Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination, their existence must have been provided for by law ...  

I note that similar concerns were the impetus for the enactment of the Canadian DPLs being discussed here, as described above in Section 2.2.2.

Gratton’s first category of privacy harms comprises harm that is subjective in nature, as it typically relates to an emotional or psychological type of harm. Calo writes that subjective privacy harm is the harm that arises from “the perception of unwanted observation, broadly defined,” which includes embarrassment, chilling effects on behaviour, and loss of solitude. Similar themes have emerged elsewhere. Ruth Gavison has written about casual observation having an “inhibitive effect on most individuals that makes them more formal and uneasy.”

Recently, the Ontario Court of Appeal in Jones v Tsige also identified a subjective aspect to privacy invasion by requiring such invasion to be “highly offensive causing distress, humiliation or anguish” before it can meet the test for Canada’s new tort of intrusion upon seclusion. As explained in greater detail below in Section 4.1.3, Gratton argues that subjective harm is the type of harm that typically arises at the point of collection and disclosure due to a “a feeling of being observed (or under surveillance).”

---

184 EC, Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector (EC, 1974) at 88.
185 Gratton, supra note 183 at 159.
186 Calo, supra note 181 at 1144-1147.
187 Gavison, supra note 93 at 447.
188 Jones v Tsige, 2012 ONCA 32.
189 Ibid. at 71.
190 Gratton, supra note 183 at 160-161.
By contrast, the second category of harm comprises harm that is objective in nature, that is, it is “external to the person harmed.”\footnote{Ibid. at 187.} Objective information-based harm entails “the forced or unanticipated use of information about a person against that person.”\footnote{Ibid. Calo, supra note 354 at 1143.} This type of harm can arise where, for example, “personal information is used to justify an adverse action against a person, as when the government leverages data mining of sensitive personal information to block a citizen from air travel, … [where] one neighbor forms a negative judgment about another based on gossip”\footnote{Gratton, supra note 183 at 187-188.}, or where personal information is used to commit a crime, such as identity theft or murder.\footnote{Ibid. at 190.}

Gratton identifies three types of objective harm. The first is financial harm, including theft and identity fraud. The second is “information inequality”, which denotes circumstances in which information is used to discriminate against an individual by, for example, removing a benefit, tarnishing his or her reputation, or denying his or her application for employment, credit, a mortgage or a loan, etc. In relation to this type of harm, Gratton highlights concerns about consumer profiling, ever more facilitated by the onslaught of Internet technologies. For example, Amazon has been suspected of using “adaptive pricing” or “dynamic pricing”, which involves using cookies to identify the profile of a specific client and raising the price of certain products based on the profile of the potential purchaser.\footnote{Ibid. at 190.} The third type of harm in this category is what Gratton calls physical harm, including stalking, rape, and murder. That Canadian DPLs aim to protect against this type of harm is reflected in, for example, the breach notification requirements
under the *Alberta PIPA* and *BC PIPA*, which require notification where harm such as this is likely to arise. Accordingly, objective privacy harm intimates “a more tangible kind of harm”, and typically arises at the point of use, which I explain in more detail below in Section 4.1.3.\(^{195}\)

Notably, although Canadian DPLs are often referred to as “privacy legislation”, and *PIPEDA* and the *Civil Code of Québec* expressly reference a “right to privacy” in their purpose provisions, the protection offered by Canadian DPLs is in fact broader than the protection of “privacy” in the strict sense. As Gratton contends, it is the protection against the *risk of harm* to an individual resulting from the collection, use and disclosure of his or her personal information.\(^{196}\) Gratton writes that this purpose “is the most logical one in the context of data protection rights, since although these rights include a privacy aspect, the type of harm that may result from the use of data is much broader than privacy harm in the strict sense” (as embodied in the first and second wave conceptions of privacy).\(^{197}\) For example, the use of inaccurate or incomplete information as the basis for a decision about an individual is a “legitimate subject for data protection” even though it does not necessarily raise questions of “privacy”.\(^{198}\) Similarly, in an article advancing a framework for structuring the current debates on privacy in the context of information technology, van den Hoven and Vermaas state that the fact that personal information is used to “inflict harm or cause serious disadvantages to individuals does not necessarily make such uses violations of a moral right to *privacy*”.\(^{199}\) An example they provide is where information is

\(^{195}\) *Ibid.* at 188.

\(^{196}\) Gratton, *supra* note 6 at 202.

\(^{197}\) *Ibid.* at 202. Here, Gratton uses the term “privacy” in a sense that invokes the first and second wave conceptions of privacy as protection against intrusions on human dignity and integrity, and on the individual’s private and family life.

\(^{198}\) *Ibid.* at 207.

\(^{199}\) Van Den Hoven & Vermaas, *supra* note 5 at 285.
collected from databases and the Internet in order to commit crimes such as identity theft. As argued by Gratton, it is ultimately the fear of this broader type of information-based harm that has prompted the development of DPLs throughout the world.

Gratton writes that this “much broader” goal of protecting against risk of harm “is evidenced in old texts pre-dating the enactment of DPLs or leading to the adoption of national laws or transnational policy documents incorporating the FIPs, as well as from more recent documents.” For example, these documents refer to electronic data processing that can be “harmful” to individuals; information that “may cause serious damage”; information that “may lead to unfair discrimination”; the retention of data that is unreasonably long and could be harmful as a result; the “retention of information that, even if not intended for use, “presents a certain risk (for example, in case of accidental leaks).” These documents also recommend that special rules should govern the processing of sensitive information “in view of the damage which individuals might suffer in case of misuse.” These are the types of concerns that the FIPs were designed to address, all of which referred to a risk of harm to an individual that could arise if his or her information was inappropriately used or disclosed.

More recently, the DPLs developed based on the type of working documents discussed above, also aim to protect individuals or personal information against risk of harm. For example, the

Footnotes:

200 Ibid.
201 Gratton, supra note 6. at 202.
202 Ibid. at 210.
203 Ibid.
204 Ibid.
205 Ibid. at 211, n 800.
EC Directive on Personal Data Protection is intended to apply to “situations where the rights of individuals are at risk.”206 In addition, Pierre Trudel argues that the underlying rationale for the implementation of DPLs is to protect individuals against the risk of harm:

In sum, the system of regulation is designed to re-establish balance between risks and precautions. It has to encourage all stakeholders to minimize the risks flowing from situations over which they have some control and to maximize the risk incurred by stakeholders who choose to behave in ways that are harmful or unduly increase risks to legitimate users. Privacy protection on the Internet belongs to this approach.207

Thus, according to these scholars, DPLs aim to regulate the risks of harm that arise when organizations collect, use and disclose personal information. As van den Hoven and Vermaas explain in presenting their taxonomy of moral reasons for justifying the protection of personal information, in developing DPLs:

… we do not want to be ‘left alone” or to be “private”, but we want more concretely to prevent others from harming us, treating us unfairly, discriminating us, [sic] or making assumptions about who we are.208

In sum, the theories advanced by privacy and information technology experts such as Gratton, van den Hoven, Vermaas and Trudel propose that the prevention of information-based harm lies at the heart of DPLs worldwide. Based on these theories, as well as the reasons that follow, I demonstrate that Canadian DPLs indeed fall within this category, and have at their heart the prevention of information-based harm.

208 Van Den Hoven & Vermaas, supra note 5 at 285.
2.4.3 Risk of Harm Principle in Canadian DPLs

That Canadian DPLs aim to prevent the types of information-based harm identified above is evidenced by the context of and reasons for their development, as described in the preceding section. For example, PIPEDA and the substantially similar provincial private sector DPLs incorporate foundational principles that were developed in response to specific concerns about the threat of information-based harm associated with rapidly developing technology.\(^{209}\) This is further evidenced in the provisions of these statutes, as well as records documenting the legislative history leading to their enactment, and the commentary of courts.

For example, in the summary of its findings, the 2000 Special Committee on Information Privacy in the Private Sector wrote that “British Columbians are in fact concerned about information privacy” and set out the types of risks about which there was concern. These included:

- lack of control over personal information\(^{210}\);
- credit card or other financial information at risk\(^{211}\);
- the possibility of increased stigmatization and discrimination based on sensitive medical information, such as genetic information\(^{212}\);
- improper use of personal information and use of personal information by unauthorized users\(^{213}\);
- judgment, criticism, and prejudice because the qualities of a person’s private life do not match the views held by others\(^{214}\);
- the impact of private sector information use on … human and civil rights\(^{215}\) and personal identity\(^{216}\),

---

\(^{209}\) Gratton, \textit{supra} note 6 at xxvii.

\(^{210}\) Report of the \textit{BC PIPA} Special Committee, \textit{supra} note 83 at 66.

\(^{211}\) \textit{Ibid.}

\(^{212}\) \textit{Ibid.} at 30.

\(^{213}\) \textit{Ibid.} at 7.

\(^{214}\) \textit{Ibid.} at 31-32.

\(^{215}\) \textit{Ibid.} at 7.

\(^{216}\) \textit{Ibid.} at 24.
• “consumers are defenseless against unauthorized collection, use and disclosure in consumer-to-business and business-to-business operations, including direct marketing, loyalty programs, credit reporting, Internet technologies, fraud and “scams”217;
• “the scope and diversity of assaults on personal privacy”218;
• personal information privacy “could be compromised by “someone finding out a lot about you”, or by computer hackers”219;
• “fear of exploitation”220;
• “information being sold to direct marketers”221;
• “big brother” knowing too much”222;
• “fear of misuse of information/ concern it will be used against me”223;
• “abuses by those who provide goods and services”224; and
• “advertisers can easily access addresses and phone numbers by browsing databases of publicly available information”, “private investigators can obtain personal information for clients whose motives are questionable”, and “third-party access to unlisted phone numbers and addresses can put individuals at risk”225.

Thus, the potential harms identified in the Report are by and large the same as or similar to the information-based harms described by Gratton, Trudel, and van den Hoven and Vermaas.

Similarly, in Alberta’s Consultation Report, participants reported concerns about the protection of their financial, credit and health information, as well as information about their country of origin and ethnic background gathered by employers, and about consumer profiling.226 For example, participants were concerned about incorrect information being held by credit agencies, the security of the information holdings and the difficulty experienced when trying to correct inaccurate information; about financial information relating to income, source of income and

217 Ibid. at 23.
218 Ibid.
219 Ibid. at 23.
220 Ibid. at 66.
221 Ibid. at 23.
222 Ibid.
223 Ibid. at 66.
224 Ibid. at 41.
225 Ibid. at 52.
226 The Alberta Consultation Report, supra note 160 at 10.
banking information; about health information including medical conditions, prescribed drugs, injuries or information that might affect one’s ability to get insurance, and about unauthorized use and third party access.\textsuperscript{227}

Reference to the risk of harm principle can also be found in the language within Canadian DPLs. For example, the \textit{BC PIPA} requires organizations to make a reasonable effort to ensure that personal information collected by or on behalf of the organization is accurate and complete, if the personal information (a) is likely to be used by the organization to make a decision that affects the individual to whom the personal information relates, or (b) is likely to be disclosed by the organization to another organization.\textsuperscript{228} As explained in the Report of the \textit{BC PIPA} Special Committee, the accuracy principle of data protection is meant to “prevent individuals from being unfairly discriminated against or harmed by inaccurate or inappropriate information”.\textsuperscript{229} Further, Canadian DPLs require organizations to protect personal information in their custody or under their control by making reasonable security arrangements to prevent harms such as unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.\textsuperscript{230} In addition to the express reference to “risks”, implicit in these provisions is the intent to protect individuals against the serious harms that may arise upon unauthorized handling or misuse of personal information.\textsuperscript{231} Further, in assessing the appropriate levels of security, organizations are expected to take into account the sensitivity of the information being safeguarded, and recognize

\begin{flushright}
\footnotesize
\textsuperscript{227} \textit{Ibid.} at 9-15.  \\
\textsuperscript{228} \textit{BC PIPA, supra} note 23, s 33.  \\
\textsuperscript{229} \textit{Report of the BC PIPA Special Committee, supra} note 83 at 37.  \\
\textsuperscript{230} \textit{PIPEDA, supra} note 15, Sch 1, Cl 4.7; \textit{Alta PIPA, supra} note 22; \textit{BC PIPA, supra} note 23, s 34; \textit{Québec Act, supra} note 21, s 10.  \\
\textsuperscript{231} \textit{Report of the BC PIPA Special Committee, supra} note 83 at 37.
\end{flushright}
that sensitive personal information may require special treatment.\textsuperscript{232} This type of requirement implies that the mishandling of information that is sensitive will be more harmful to individuals than other types of personal information.

The commentary of courts further demonstrates that a fundamental purpose of Canadian DPLs is to protect against the risk of information-based harm. Recently, the Supreme Court of Canada stated that both the \textit{Alberta PIPA} and \textit{PIPEDA} “are part of an international movement towards giving individuals better control over their personal information”\textsuperscript{233} describing the purpose of the \textit{Alberta PIPA} as follows:

The purpose of \textit{PIPA} is explicitly set out in s. 3, as previously noted … The focus is on providing an individual with some measure of control over his or her personal information: Gratton, at pp. 6 ff. The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy.

\textit{PIPA}’s objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others for their own purposes. There is also no serious question that \textit{PIPA} is rationally connected to this important objective.

The beneficial effects of \textit{PIPA}’s goal are demonstrable. \textit{PIPA} seeks to enhance an individual’s control over his or her personal information by restricting who can collect, use and disclose personal information without that individual’s consent and the scope of such collection, use and disclosure. \textit{PIPA} and legislation like it reflect an emerging recognition that the list of those who may access and use personal information has expanded dramatically and now includes many private sector actors. \textit{PIPA} seeks to regulate the use of personal information and thereby to protect informational privacy, the foundational principle of which is that “all information about a person is in a fundamental way his own, for him to communicate or retain . . . as he sees fit” …

Insofar as \textit{PIPA} seeks to safeguard informational privacy, it is “quasi-constitutional” in nature… The importance of the protection of privacy in a vibrant democracy cannot be overstated… As Chris D. L. Hunt writes in “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy

\textsuperscript{233} 
\textit{AIPC v UFCW, supra} note 169 at para 13.
Tort” …, “[d]emocracy depends on an autonomous, self-actualized citizenry that is free to formulate and express unconventional views. If invasions of privacy inhibit individuality and produce conformity, democracy itself suffers.”

PIPA also seeks to avoid the potential harm that flows from the permanent storage or unlimited dissemination of personal information through the Internet or other forms of technology without an individual’s consent.

Finally, as discussed above, the objective of providing an individual with some measure of control over his or her personal information is intimately connected to individual autonomy, dignity and privacy, self-evidently significant social values.234

Similarly, the Alberta Court of Appeal has also stated that the Alberta PIPA aims to protect against harms such as identity theft and the financial harm that can result.235 This, together with the examples set out above, demonstrates that Canadian DPLs indeed seek to protect against the risk of information-based harms, such as embarrassment or humiliation from the sharing of “intimate” information (e.g., medical information), financial harm (e.g., from unauthorized access to bank accounts and credit card information), adaptive pricing, adverse treatment of an employee by an employer, identity theft, and even physical harm caused by violence.

234 Ibid. at paras 19-24.
Chapter 3: Critique of Existing Interpretations of “Personal Information” under Canadian DPLs

In this chapter, first I review the main approaches used under Canadian DPLs to interpret “personal information”. I then critique these approaches and argue that they are inadequate in light of the fundamental purpose of these statutes to protect only data that poses a risk of information-based harm, and that a new uniform approach is justified in light of technological and societal change.

3.1 Expansionist Approaches to Interpreting “Personal Information” in Canada

As discussed above, the Alberta PIPA, BC PIPA and PIPEDA all define personal information as “information about an identifiable individual”. The DPL in Québec defines it as “any information which relates to a natural person and allows that person to be identified”. Accordingly, the statutory definitions of “personal information” in Canadian DPLs are identical or virtually identical, with the key element being “identification” or “identifiability”. The dominant approaches to interpreting this term under Canadian DPLs have been what I will call “expansionist”. Schwartz and Solove use this descriptor in describing the EU’s approach to defining “personal information”, in contrast to the United States’ reductionist approach. Under the latter interpretive approach, “the tendency is to consider [“personally identifiable information”] as only that personal data that has been specifically associated with a specific person.”236 Thus the reductionist model protects only identified data, and “thereby leaves too

much personal information without legal protections”. By contrast, in the expansionist approach, “it is irrelevant if information has already been linked to a particular person, or might be so linked in the future; this view treats identified and identifiable data as equivalent.” As various authors have underscored, the interpretation used under Canadian DPLs reflects the influence of the EU’s expansionist approach and “goes even further in dropping the concept of “identified” in its approach to [“personally identifiable information”].”

As explained below, two very similar expansionist approaches have been adopted in the interpretation of “personal information” under Canadian DPLs. Decision-makers interpreting this term under PIPEDA, the Québec Act and the Alberta PIPA use a broad literal approach. Recently in Schindler Elevator, the BC Privacy Commissioner adopted what I will call a “relative” version of the broad literal approach. Below, I discuss these two expansionist approaches in greater detail in order to provide the context for evaluating them and arguing in favour of a new, purposive risk of harm based approach.

3.1.1 The Broad Literal Approach under PIPEDA, the Québec Act and Alberta PIPA

The PIPEDA defines “personal information” broadly as “information about an identifiable individual”. The approach taken to interpreting “personal information” under PIPEDA is a literal reading, in the sense that the statutory definition “information about an identifiable individual” is

237 Ibid.
238 Ibid.
239 Ibid.
240 Schindler Elevator Corporation, [2012] BCIPC No 25 [Schindler Elevator].
given its ordinary or common meaning.\textsuperscript{241} Under this interpretation, it is not necessary to show that the information relates to one’s dignity or integrity, or connotes notions of intimacy and personal identity. Information is interpreted to meet the definition under \textit{PIPEDA} when it is or can be linked to a specific individual whose identity can be discerned. In its “Interpretation Bulletin”\textsuperscript{242} respecting the meaning of “personal information”, the OPCC explicitly identifies the following principles drawn from Canadian case law as material to its interpretation of that term:

a) The definition of personal information must be given a broad and expansive interpretation;\textsuperscript{243}

b) Personal information is information “about” an identifiable individual. “About” means that the information is not just the subject of something but also relates to or concerns the subject;\textsuperscript{244}

c) Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information;\textsuperscript{245}

d) Information will still be personal information even if it is publicly available within the meaning of the regulations, and is exempt from applicable consent requirements;\textsuperscript{246}

\begin{itemize}
  \item\textsuperscript{241} See Pierre-André Côté, \textit{The Interpretation of Legislation in Canada}, 4th ed ed (Toronto: Thomson Reuters Canada Ltd., 2011) at 277, in which “ordinary or common meaning” is described as “the natural meaning that appears when the provision is simply read through as a whole.” See also Gratton, \textit{supra} note 6 at 92, n 201, where the author describes a literal interpretation as an “interpretation that is based on the exact wording” of the phrase in question.
  \item\textsuperscript{242} \textit{Personal Information}, Interpretation Bulletin (Office of the Privacy Commissioner of Canada, 2013), online: <https://www.priv.gc.ca/leg_c/interpretations_02_e.asp> (accessed 24 September 2015).
  \item\textsuperscript{243} \textit{Dagg v Canada (Minister of Finance)}, 1997 SCR 403; \textit{Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)}, 2006 FCA 157, leave to appeal denied, [2006] SCCA No 259 [\textit{NAV Canada}].
  \item\textsuperscript{244} \textit{NAV Canada, supra} note 243.
  \item\textsuperscript{245} \textit{Gordon v Canada (Health)}, 2008 FC 258.
  \item\textsuperscript{246} \textit{England}, \textit{supra} note 168.
\end{itemize}
e) Subjective information about an individual may still be personal information even if it is not necessarily accurate.\textsuperscript{247}

The OPCC has in fact explicitly stated in its annual report to Parliament that “[t]he definition is deliberately broad”, that in its findings it has “tended to interpret it as broadly as possible”, and that it is “inclined to regard information as personal even if there is the smallest potential for it to be about an identifiable individual.”\textsuperscript{248} As highlighted by McIsaac et al.\textsuperscript{249}, information that has been found to constitute personal information under \textit{PIPEDA} includes NetBIOS information contained on a personal computer\textsuperscript{250}; a mobile messenger service customer’s device identifier information, mobile subscriber ID, mobile country code and mobile network code\textsuperscript{251}; GPS data\textsuperscript{252}; and “payload” data collected inadvertently from unsecured WiFi networks\textsuperscript{253}.

The OPCC’s interpretation of “information about an identifiable individual” is so broad that numerous privacy experts have remarked that “[i]n essence, almost any information in any form that can be attributed to an identified individual is caught by this expansive definition”\textsuperscript{254} and that the definition is “limitless”\textsuperscript{255} in terms of what information it can capture.\textsuperscript{256}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{247} Lawson v Accusearch Inc, 2007 FC 125.
\item \textsuperscript{248} George Radwanski, \textit{Annual Report to Parliament 2001-2002} (Ottawa: The Privacy Commissioner of Canada) at 56.
\item \textsuperscript{249} McIsaac, Shields & Klein, \textit{supra} note 17 at 4.1.1.
\item \textsuperscript{250} \textit{PIPEDA Case Summary} \#2001-25, 2001.
\item \textsuperscript{251} \textit{PIPEDA Report of Findings} \#2013-001, 2013.
\item \textsuperscript{252} \textit{PIPEDA Case Summary} \#351, 2006.
\item \textsuperscript{253} \textit{PIPEDA Report of Findings} \#2011-001, 2011.
\item \textsuperscript{254} McIsaac, Shields & Klein, \textit{supra} note 17 at 4.1.1.
\item \textsuperscript{255} Perrin et al, \textit{supra} note 168 at 54.
\item \textsuperscript{256} Gratton, \textit{supra} note 183 at 115-116.
\end{itemize}
\end{footnotesize}
Québec’s private sector DPL also defines “personal information” broadly as “any information which relates to a natural person and allows that person to be identified.” Québec’s Commission d’accès à l’information (Québec CAI) has “confirmed that any and all information that may, directly or indirectly, identify and relate to a given person is deemed to be personal information.” The CAI has also ruled that personal information is information that: (i) permits someone to learn something; (ii) relates to a natural person; and (iii) is capable of identifying the person. Accordingly, the Québec Superior Court has stated that the definition of personal information in the provincial Act is similar to the definition in PIPEDA. Some commentators argue, however, that the interpretation of “personal information” is even more expansive than the approach taken under the federal Act. For example, unlike the OPCC, the CAI has not generally excluded “business contact information” or “work product information” from the scope of the Québec Act’s definition. In addition, unlike under other Canadian DPLs, the Québec Act has not been interpreted to exclude from its scope personal information that may be otherwise publicly available.

The approach taken in Alberta is also a broad literal reading. The definition of “personal information” in the Alberta PIPA is identical to the definition in the BC Act: it is broadly defined as “information about an identifiable individual”. The Alberta Court of Appeal recently observed that the definition of personal information in the Alberta PIPA is particularly broad and that “[i]t

257 McIsaac, Shields & Klein, supra note 17 at 4.5.5.
258 Ségal v Centre de services sociaux de Québec, [1988] 1 CAI 186.
259 Air Canada c Constant, [2003] IQ 11619 (Que SC).
261 Ibid. at 266-267.
262 Ibid. at 267-268.
covers all personal information of any kind, and provides no functional definition of that term.\textsuperscript{263}

The Alberta OIPC interprets the definition of personal information expansively as information that itself can identify an individual, or that is about an individual who can be identified when linked to some form of identifier. For example, in a guide for business organizations, Service Alberta and the Alberta OIPC state:

\textit{Personal information} means information that can identify an individual (for example, name, home address, home phone number, e-mail address, ID numbers), and information about an individual (for example, physical description, educational qualifications, blood type). For PIPA to apply, the personal information in question must be about an individual, identify an individual, or be able to identify an individual.\textsuperscript{264}

The Alberta Court of Appeal in \textit{Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)}\textsuperscript{265} recently framed the Alberta approach as follows:

The “identifiable individual” term has two components. Firstly, the individual must be “identifiable”. Generic and statistical information is thereby excluded, and the personal information (here the relevant number) must have some precise connection to one individual. Secondly, the information must relate to an individual. Information that relates to objects or property is, on the face of the definition, not included. The key to the definition is the word “identifiable”. The Act is designed to regulate and protect information that is uniquely connected to one person. An important (although not the only) purpose of the Act is to control the use of information that would enable “identity theft”, that is, information that is used to distinguish one individual from another in financial and commercial transactions. This can be seen by reviewing the type of information that is dealt within the more specific provisions and exceptions in the Act. The definition is not primarily aimed at information about that individual’s opinions, choices and status in life.

Further, to be “personal” in any reasonable sense the information must be directly related to the individual; the definition does not cover indirect or collateral information. Information that relates to an object or property does not become information “about” an individual, just because some individual may own or use that property. Since virtually every object or property is connected in some way with an individual, that approach would make all identifiers “personal” identifiers. In the context of the statute, and given the purposes of the statute set out in s. 3, it is not reasonable to expand the meaning of “about an individual” to include references to objects that might

\textsuperscript{263} United Food and Commercial Workers, Local 401 v Alberta (Attorney General), 2012 ABCA 130 at para 77.


\textsuperscript{265} Leon’s Furniture Limited v. Alberta (Information and Privacy Commissioner), supra note 235.
indirectly be affiliated or associated with individuals. Some identification numbers on objects may effectively identify individuals. Many, however, are not “about the individual” who owns or uses the object, they are “about the object”.266

The case in Leon’s Furniture involved a complaint about an organization that collected driver's license and license plate information from individuals picking up products at its retail locations. The retailer argued that the information it collected did not constitute “personal information” under the Alberta PIPA. The Court of Appeal unanimously decided that driver's license numbers are “personal information”, but diverged on the question of whether vehicle license plate numbers qualified as such. The majority ruled that they did not, on the basis that license plates are "about" the vehicle, not “about” the individual who owns or uses the vehicle. The majority further stated that it would be “contrary to common sense to hold that a vehicle license number is in any respect private” since all vehicles operated on Alberta highways must display their license plates in a visible location. Although in this way the Court seemed to import into the analysis a “reasonable expectation of privacy” consideration, the Supreme Court of Canada recently emphasized that the Alberta Privacy Commissioner “has made it clear that personal information includes information that is not “private”, so that “personal information does not lose its character as personal information if the information is widely or publicly known”.

In Order F2012-14268, the Alberta OIPC considered whether records relating to water well testing contained personal information about individuals, or if the information was only “about” property. The adjudicator surveyed several decisions of the Ontario Information and Privacy

266 Ibid. at paras 47-48.
267 AIPC v UFCW, supra note 169 at para 15.
Commissioner, as well as past Orders of his office. He commented on _Leon's Furniture_ and the _Alberta PIPA_’s definition of personal information as follows:

What I glean from the foregoing relevant commentary is that a legal land description is not itself personal information: see _Leon's Furniture Ltd. v. Alberta (Information and Privacy Commissioner)_ and Ontario Order MO-2053, __. However, a legal land description may serve as an identifier that will reveal what does constitute personal information: see the various Orders cited within Ontario Order MO-2053, which concludes that "the common thread in all these orders is that the information reveals something of a personal nature about an individual or individuals". The distinction between what is and is not personal information is demonstrated in Ontario Order PO-2900, __: the fact that an individual -- who can be identifiable by virtue of information about property -- drilled a well is his or her personal information, but information about the well itself is not his or her personal information.

Consistent with the foregoing commentary are principles articulated by earlier Orders of the Office. When determining whether information is about an identifiable individual, one must look at the information in the context of the record as a whole, and consider whether the information, even without personal identifiers, is nonetheless about an identifiable individual on the basis that it can be combined with other information from other sources to render the individual identifiable __ Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information [...] citing _Gordon v. Canada (Minister of Health)_ ...].__

Similarly, in Order P2012-01__, the Director of Adjudication stated:

It is not inconsistent with _[Leon's]_ to say that in a case where the location of a property is associated with an individual in such a manner that it indicates where they reside, for example, where it is given or designated as a person's home address, the information does not merely "relate to an object or property", it relates to the individual, and it is information "about" that individual. The information is not about the person "just because" they may own the property, it is their personal information because it indicates where they live.__

In Order F2013-53__, the Adjudicator explained that whether or not information about an object or property is or is also information about an individual depends on context:

I do not understand the Court in _Leon's_ to be saying that information about property can never also be information about an individual such that it is also personal information. In my

269 Ibid. at paras 48-49 [citations omitted].
270 Order P2012-01, 2012 AIPCD No. 7.
271 Ibid. at para 21.
view, the comments of the Court do not lead to the conclusion that the broad definition of personal information specifically excludes information about property owned by an individual in any context. …

In many cases the determination as to whether information is "personal information" is dependent on the context in which it appears. A statement that a property owner does not remove snow from the sidewalk adjacent his or her property seems to be a statement about the actions (or lack of action) of the property owner, rather than a statement about the property. Similarly, a statement about an owner's landscaping or gardening practices seems to be a statement about that owner's use of her property. In comparison, a statement about the lot grading of a property or a statement about the amount of snow on a sidewalk, appear to be statements about property (although it may relate to the property owner).

Another distinction that has been made in past orders between information related to an individual and personal information about the individual is whether there is a "personal dimension" to the information. The adjudicator in Order F2010-011 commented that information about an individual's business may be personal information about that individual in circumstances that give a "personal dimension" to that information, such as allegations of wrongdoing. Similarly, information about employees acting in the course of their job duties is normally not considered information about those individuals; however, there may be circumstances that give that information a “personal dimension”, such as disciplinary issues or performance evaluations…

The Adjudicator’s interpretation of the law and decision in Order F2013-53 was upheld in

*Edmonton (City) v. Alberta (Information and Privacy Commissioner)*274, in which the Alberta Court of Queen’s Bench commented as follows:

I note that Justice Conrad in dissent in *Leon's Furniture* endorsed the broad approach to the interpretation of "personal information." The majority did not state that her discussion of the interpretation of this term was erroneous or inaccurate (see para 35 of the majority reasons). Justice Conrad reported the following at para 106:

[106] The Ontario courts have also interpreted the phrase "information about an identifiable individual", as found in Ontario's *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F31, and concluded that a broad interpretation is required. In *Ontario (Attorney General) v Ontario (Information and Privacy Commissioner)* … (aff'd *Ontario (Attorney General) v Pascoe* …), the Ontario Superior Court of Justice (Divisional Court) considered whether doctors' billing information qualified as "information about an identifiable individual". The question in the case was not whether billing information was information "about" a doctor. Rather, the issue related to whether individual doctors could be identified from the information so that the information

---

273 *Ibid.* at paras 43, 47-48 [citations omitted].
274 *Edmonton (City) v Alberta (Information and Privacy Commissioner)*, 2015 ABQB 246.
amounted, in each case, to information about an identifiable individual. In this context, the court held that any information which, when combined with other information, could identify a person, amounted to information about an identifiable individual under the statute. The court stated at paras 14-15:

"If there is a reasonable expectation that the individual can be identified from the information, then such information qualifies under subs. 2(1) as personal information." …

The test then for whether a record can give personal information asks if there is a reasonable expectation that, when the information in it is combined with information from other sources otherwise available, the individual can be identified. A person is also identifiable from a record where he or she could be identified by those familiar with the particular circumstances or events contained in the record. ... 275

Taking into account that some case law suggests that the definition of personal information is narrowed and a broad interpretation is not appropriate, the Court endorsed the broad literal approach, stating: “With the very greatest of respect, a broad interpretation of “personal information” is consistent with the authorities.” 276

Thus the dominant approach to interpreting the term “personal information” under PIPEDA, the Alberta PIPA and the Québec Act is decidedly a broad literal approach in all three jurisdictions. It is the first type of expansionist interpretive approach discussed herein.

275 Ibid. at para 50 [citations omitted].
276 Ibid. at para 51.
3.1.2 The Relative Approach under the BC PIPA

The BC Information and Privacy Commissioner recently ruled in Schindler Elevator\textsuperscript{277} that under the BC PIPA, “personal information” is to be interpreted using a slightly modified, more relative, version of the OPCC’s broad literal approach described above. In Schindler Elevator, the BC Commissioner investigated a complaint brought by a group of employees who objected to their employer’s use of a GPS system to monitor company vehicles. The technology recorded data such as vehicle location and information about the manner in which the vehicle was being driven, generating reports only where the vehicle’s use deviated from accepted norms. Schindler Elevator’s reasons for collecting the information included managing productivity and hours of work, as well as ensuring employees were driving safely.

The complainants claimed the data generated by the GPS was “personal information” under the BC PIPA, and that the organization’s collection and use of that information violated the Act. They argued that the Commissioner ought to follow the literal approach adopted in cases such as PIPEDA Summary #351\textsuperscript{278}. By contrast, Schindler Elevator contended that the appropriate approach to defining personal information was the privacy-based interpretation applied in the leading case, Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)\textsuperscript{279} (NAV Canada). The company argued that the disputed information was “about” the vehicle and not “about” the employee driving it. The BC Commissioner rejected the organization’s position, expressly refusing to adopt the privacy-based interpretation of “personal information” endorsed in cases such as NAV Canada. In her view,

\begin{footnotesize}
\begin{enumerate}
\item Schindler Elevator, supra note 240.
\item PIPEDA Case Summary #351, supra note 252.
\item NAV Canada, supra note 243.
\end{enumerate}
\end{footnotesize}
personal information is not limited to information about an individual’s “personal” or “private” life.\textsuperscript{280} She stated:

Nothing in PIPA suggests that ‘personal' information was intended to be confined to a personal zone of privacy or intimacy outside or within the worlds of work and commerce. Rather, the purposes of PIPA are achieved by a definition of personal information that facilitates the mandated balancing of the interest in protecting it with the interest in using it in accordance with the legislatively-prescribed standards.\textsuperscript{281}

In the result, the Commissioner interpreted “personal information” under the \textit{BC PIPA} broadly as:

\begin{quote}
… information that is reasonably capable of identifying a particular individual, either alone or when combined with other available sources of information, and is collected, used or disclosed for a purpose related to the individual.\textsuperscript{282}
\end{quote}

Information falling within this interpretation may include information that has multiple purposes (\textit{e.g.}, mileage information about a company vehicle may be used for asset management as well as employee discipline).\textsuperscript{283}

The approach to interpreting “personal information” articulated in \textit{Schindler Elevator} narrows the broad literal approach to a small extent by adding a contextual consideration of the purpose for which the information in question is collected, used or disclosed. This approach is akin to what Robinson \textit{et al.} call a “more relative interpretation” in discussing the approach advanced by

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{280} \textit{Schindler Elevator}, supra note 240 at para 83.
\item \textsuperscript{281} \textit{Ibid.} at para 49.
\item \textsuperscript{282} \textit{Ibid.} at para 85.
\item \textsuperscript{283} \textit{Ibid.} at para 83.
\end{itemize}
\end{footnotesize}
the Article 29 Working Party\textsuperscript{284} for the interpretation of “personal data” under the \textit{EC Directive on Personal Data Protection}. They write:

A more relative interpretation of personal data was recently described in Opinion No 4/2007 of the Article 29 Working Party, which noted that, in order to find that data “relate” to an individual, either a "content" element, a "purpose" element or a "result" element should be present. This means that data is personal data when it contains information about a specific person (content), when it is used or likely to be used to determine the treatment of a specific person (purpose), or when it is likely to have an impact on a specific person (result).\textsuperscript{285}

Since the \textit{Schindler Elevator} approach closely resembles the approach described above, I have in this thesis called it the “relative approach” or “relative interpretation”. It is the second type of expansionist approach discussed herein.

In sum, decision-makers interpreting “personal information” under the PIPEDA, Québec Act and \textit{Alberta PIPA} take a broad literal approach. The BC OIPC favours a slightly narrower version of the broad literal approach, \textit{i.e.}, the relative approach. Both of these are expansionist interpretive approaches, and I will refer to them collectively as such throughout this thesis.

\subsection{3.2 Critical Appraisal of the Existing Approaches to Interpreting “Personal Information”}

As discussed above, Canadian DPLs define “personal information” as “information about an identifiable individual” and, in Québec, “information which relates to a natural person and allows that person to be identified”. Canada’s privacy commissioners and courts interpret this definition expansively to include any information that, either alone or in combination with other

\textsuperscript{284} \textit{Opinion 4/2007}, \textit{supra} note 206 at 10. In 2007, the Article 29 Working Party, a key advisory body to the European Union Commission, issued this opinion on the definition of “personal data” under the \textit{EC Directive on Personal Data Protection}, proposing a more relative interpretation of the definition.

\textsuperscript{285} Robinson et al, \textit{supra} note 182 at 27 [footnotes omitted].
information, can identify or be linked or connected to a specific individual. For the reasons that follow, I argue that the existing approaches to interpreting “personal information” frustrate the fundamental goal of Canadian DPLs, which is to facilitate the free flow of information for trade and commerce while protecting individuals against the risk of information-based harm, such as embarrassment or humiliation from the disclosure of “intimate” information (e.g., medical information), financial harm (e.g., from unauthorized access to bank accounts and credit card information), adaptive pricing, adverse treatment of an employee by an employer, identity theft, and even physical harm caused by violence. The framework I use for this purpose is based on the work of Lyria Bennett Moses, as modified by Gratton. Moses has identified four main reasons for which laws are seen to necessitate reform due to technological development. In her book, Gratton frames her criticisms against the literal definition of “personal information” under European and Canadian DPLs around three of Moses’s rationales for reform. These are:

1. Over-inclusiveness and Under-inclusiveness: “Where existing legal rules were not formulated with new technologies in mind, those rules may inappropriately include or exclude new forms of conduct”; 
2. Uncertainty: “The law may be uncertain as it applies to new forms of conduct. In other words, it may not be clear whether such conduct is commanded, prohibited, or authorized. Existing legal rules may need to be clarified”; and

287 Gratton, supra note 6 at 92. Bennett Moses discusses four legal problems arising from technological change, the fourth being “the potential need for special laws to ban, restrict or, alternatively, encourage a new technology”; however, Gratton adopts a framework centred on the three problems listed here.
288 Bennett Moses, supra note 286 at 16.
289 Ibid.
3. Obsolescence: “Some existing legal rules may be justified, explicitly or implicitly, on the basis of a premise that no longer exists.”

I use the same framework to argue that the expansionist interpretations of the definitions of personal information under Canadian DPLs frustrate the fundamental goal of these statutes.

3.2.1 Over-inclusiveness and Under-inclusiveness

First, these approaches may lead to over-inclusiveness and under-inclusiveness in light of the DPLs’ purpose to protect only information that poses a risk of harm to the individual who has been or can be identified through, or in relation to, the information in question. As stated by Omer Tene, these types of frameworks for interpreting the term “personal information” are “either overbroad, potentially encompassing every bit and byte of information, ostensibly not about individuals; or overly narrow, excluding de-identified information, which could be re-identified with relative ease.”

Under expansionist approaches in use under Canadian DPLs, information will be “about” an individual not only when he or she is the subject of that information, but also when that information relates to or concerns that individual. The individual will be “identifiable” where there is a serious or reasonable possibility that he or she could be identified through the use of that information, alone or in combination with other information. As a result, the existing interpretations run a serious risk of being over-broad and over-inclusive, because they will encompass any information that can be directly or indirectly linked to a specific individual, whether or not its collection, use or disclosure may be harmful to that person,

290 Ibid.
291 Tene, supra note 9 at 1219.
or is worthy of protection. Boštjan Berčič and Carlisle George provide the following example of such over-breadth:

… the fact that a piece of land X that is owned by James Moore is worth €100,000 is … personal data. At first sight a value of a piece of land or an object is not personal data, but it becomes one as soon as it is (in any way) related to an individual. Similarly, for example, the fact that the water on the piece of land is potable (or not) can become personal data if we know whose piece of land it is or who lives on it. Many other absurd examples like this can be constructed (e.g., the fact that Paris is the capital of France can become personal data if we relate it to John Smith who lives in Paris, the capital of France). 292

Further, as Schwartz and Solove have noted, expansionist approaches are flawed because they treat data about identifiable and identified persons as conceptually equivalent. 293 The difficulties they identify are “that there is a broad continuum of identifiable information that includes different kinds of anonymous or pseudonymous information” and also that “[d]ifferent levels of effort will be required to identify information, and varying risks are associated with the possible identification of data.” 294 To place all such data into the same conceptual category as data that currently relate to an identified person, they say, is “a blunt approach”. 295 This risk of over-breadth is particularly applicable with respect to developing technologies. As Paul Ohm has written: “No matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered.” 296 He aptly cautions that the list of potential

---

293 Schwartz & Solove, supra note 236 at 1876.
294 Ibid. at 1876.
295 Ibid. at 1876.
296 Ohm, supra note 10 at 1742.
“personally identifiable information” (PII) will “never stop growing until it includes everything.”

I argue that the risk of this type of overbreadth can equally result from the *Schindler Elevator* relative interpretation in BC, even though it is limited to a certain extent by the second element of the Commissioner’s interpretation (i.e., which relates to the purpose for which the information is collected, used or disclosed). While this element results in greater flexibility than provided for in a strict literal interpretation, it is still very broad and may still create over-inclusiveness as a result. Gratton advanced a similar criticism about the relative interpretation proposed by the Article 29 Working Group (as discussed in the preceding section), drawing from the work of Neil Robinson et al., who wrote:

> A more relative interpretation of personal data was recently described in Opinion No. 4/2007 of the Article 29 Working Party, which noted that, in order to find that data “relate” to an individual, either a "content" element, a "purpose" element or a "result" element should be present. This means that data is personal data when it contains information about a specific person (content), when it is used or likely to be used to determine the treatment of a specific person (purpose), or when it is likely to have an impact on a specific person (result). Thus, IP addresses, user names or maps might not always be classified as personal data, the context within which the data is processed must be examined to determine whether one of the three criteria have been met.

Determining what constitutes personal data becomes particularly acute in the context of mobile telecommunications, where a device with an IP address may easily be used by another entity. The problem is likely to get worse with IPv6, when IP addresses will become much more widely available and begin to be assigned to objects such as home appliances or cars.

While the relative interpretation is more flexible than the absolute one, the three criteria are still very broad. For instance, a website that uses IP addresses to determine the likely origin of a visitor for language customization purposes clearly uses information “to determine the treatment of a specific person” and “to have an impact on a specific

298 Gratton, *supra* note 6 at 111.
person”. Thus, data protection rules would apply, regardless of the apparent lack of privacy risk.\textsuperscript{299}

What may result from such an overly broad interpretation of “personal information” is the enforcement of data protection obligations that, if breached, do not even pose a risk of the information-based harm against which the DPLs actually aim to protect.

Privacy and information technology experts such as Vincent Gautrais, Pierre Trudel, Karim Benyekhlef, Paul Ohm, and Gratton discuss a number of undesirable consequences that may flow from an over-inclusive definition in this context. First, such over-inclusiveness creates a burdensome framework, “resulting in a system in which organizations and industry players incur additional costs for complying with DPLs that have nothing to do with the protection of individuals.”\textsuperscript{300} In addition, an overreaching definition creates a situation where “all kinds of definitions” need to be carved out for the public good.\textsuperscript{301} Third, an over-reaching definition capturing personal information that does not even pose a risk of harm will lead to the unjustifiable regulation of “too many situations”, and as a result, “organizations may be less and less inclined to comply with the law, if such law does not properly reflect the factual reality”.\textsuperscript{302} Fourth, an overly broad definition “may trigger a system in which organizations and industry players will incur additional costs for complying with DPLs, which have nothing to do with the

\textsuperscript{299} Robinson et al, \textit{supra} note 182 at 27-28 [footnotes omitted].

\textsuperscript{300} Gratton, \textit{supra} note 6 at 105.

\textsuperscript{301} \textit{Ibid.} at 105. Gratton draws from Pierre Trudel & Karim Benyekhlef, “Approches et Strategies pour Ameliorer la Protection de la vie Privee dans le Contextes Inforoutes” (Montreal: CRDP, Universite de Montreal, 1997) at 11.

protection of individuals”.

In my view, all of these likely consequences make existing expansionist approaches unworkable.

In addition, the relative inflexibility of these approaches may lead to under-inclusiveness by failing to cover information that ought to be protected in light of the DPLs’ purpose.

The existing approaches may result in the exclusion of new types of data because they relate to a device or an object (not an individual), or because the identity (e.g., name or contact information) is unknown or very difficult to ascertain, even though the data are meant to be covered by the DPLs.

For example, requiring data to be “capable of identifying” an individual may result in a failure to protect the individual against harms such as profiling and behavioural marketing techniques.

Profiling can involve the inference of a set of characteristics about a relatively abstract category of persons (e.g., male university students), and these characteristics are then employed to assess persons who belong to that category.

Another form of profiling involves the inference of a set of characteristics about a specific individual on the basis of collection and analysis of data related to that person, as opposed to data related to other persons or an abstract category of persons. In practice, these two forms of profiling often overlap, that is, abstract profiles are often generated partly on the basis of specific profiling and vice versa.

As Lee Bygrave explains, for the purpose of abstract profiling, none of the data used to generate the profile needs

303 Gratton, supra note 6 at 105.
304 Gratton, supra note 183, at 120.
306 Ibid.
307 Ibid.
to be capable of revealing the identity of a specific person; they can be, “from the viewpoint of data protection laws, completely non-personal”.  

With respect to specific profiling, although this form of profiling tends to require the existence of some data that are capable of being connected to a unique person, Internet profiles can be generated merely on the basis of net-browsing patterns (registered as clickstream data and often stored in part as cookies) that are directly linked to the user’s hardware and software as opposed to, for example, the user’s own name or Personal Identification Number (PIN). As a result, due to the focus on “identifiability” in the existing interpretations, certain profiles may be considered anonymous and not covered under the definition of “personal information” under Canadian DPLs. For example, take the allegation that Amazon uses profiling to practice “adaptive pricing” by using cookies that raise the price of certain products depending on the profile of the potential purchaser. These profiles may be considered anonymous and thus excluded from the definition if the identity of the individual affected by the adaptive pricing is unknown, even though this individual is subject to some type of discrimination or other type of harm that DPLs were intended to address. As a result, information worthy of protection in furtherance of the DPLs’ fundamental purpose may in such circumstances be exposed. I argue in concurrence with Gratton that these likely consequences of the relatively inflexible existing approaches weigh in favour of adopting a new, more flexible and nuanced approach that focuses on the purpose DPLs aim to fulfill.

308 Ibid. at 304.
309 Ibid.
310 Gratton, supra note 6 at 107.
3.2.2 Uncertainty

In relation to the second consideration in the Bennett Moses/Gratton framework, the existing expansionist approaches may result in uncertainty due in particular to new types of data and collection tools. Uncertainty poses a problem in this context because it can cause organizations subject to data protection legislation to be uncertain whether the information they are handling qualifies as “personal” such that it triggers their data protection obligations.

In order to qualify as personal information under existing expansionist interpretations, the information must be reasonably or seriously capable of identifying or being connected to a specific individual. Therefore, if an organization has information about an individual, but it is impossible (or very difficult) for the organization to determine who that individual is, then uncertainty can arise about whether the information is “personal information”, and whether the organization’s data protection obligations are triggered as a result. The disagreement over how to characterize Internet Protocol (IP) addresses for the purposes of applying DPLs illustrates the uncertainty over new types of data. Every computer connected to the Internet receives a unique IP address that enables communication with other computers.312 As part of the normal data exchange, Web servers record, or “log”, these addresses for future network and security analysis.313 These logs can provide a “breadcrumb trail of a user’s online activity”, including when he or she views a Web site, posts on a blog, views a sexually explicit photograph, or reads a political article.314 Although “these logs are scattered across the vast reaches of the Internet,

313 Ibid.
314 Ibid.
there are important middlemen with access to it all: Internet Service Providers (ISPs).” ISPs assign IP addresses to their subscribers, logging who is using what address at any given time. By comparing its own IP address logs to those maintained by the Internet's Web servers, an ISP can link online activity to a specific subscriber account and, potentially, to an individual. In 2013, through conducting a simple test, the OPCC determined that knowledge of an IP address allows a searcher to obtain other information about a network, device or service, enabling the searcher to expose, for example, peer-to-peer (P2P) activities (e.g., file sharing), records in web server log files, or glimpses of the individual’s web activities (e.g., Wikipedia edits). These “bits of individuals’ online history may reveal their political inclinations, state of health, sexuality, religious sentiments and a range of other personal characteristics, preoccupations and individual interests”.

There is distinct disagreement between and within Europe, the US and Canada on whether or not IP addresses constitute personal information for the purposes of DPLs. In the American context, for example, although some companies have successfully argued in court that an IP address is not personal information, Joshua McIntyre contends that IP addresses are functionally similar to other types of personal information and should accordingly be protected when in the hands of an ISP or otherwise correlated to identifying information. Similarly, in Europe, even within the same jurisdiction in some instances, courts have disagreed on whether IP addresses are

315 Ibid. at 897.
316 Ibid.
317 Ibid.
319 Schwartz & Solove, supra note 236 at 1838-1839.
320 McIntyre, supra note 312.
personal information, due mainly to inconsistencies in how the expansionist interpretation of personal information was applied. In Canada, the OPCC takes the position that an IP address can constitute personal information if it can be associated with an identifiable individual, which has also resulted in uncertainty and questionable outcomes, even within a single case. For example, in *PIPEDA Case Summary #319 (IS Provider)*, the Assistant Commissioner accepted that an originating IP address qualified as “personal information” but that a destination address did not based on the possibility of the individual behind each being identified.

Similar inconsistencies resulting from the application of expansionist approaches have arisen within Canada in relation to, for example, licence plate numbers and location information (as discussed in greater detail below in Section 4.2.1.1). With respect to the former, in Québec, the courts have taken the position that license plate numbers should be considered personal information. At the federal level, the OPCC has implied that license plate numbers should qualify as personal information by stating that “organizations should not collect unique identifying numbers appearing on government-issued documents (driver's licences, health cards, licence plates, etc.), for purposes other than those intended by the issuers of these documents.”

In Alberta, in Investigation Report F2008-IR-002, the Alberta OIPC found that where a vehicle is owned by an individual (as opposed to a corporation), the licence plate number is personal information. This view, however, is not unanimously held throughout Canada, or even in the same jurisdiction in the case of Alberta. In 2011, in the appeal of a lower court

---

323 Gratton, *supra* note 183 at 139, Fn 171. See for example *Syndicat de Autobus Terremont Ltee c Autobus Terremont Ltee et Paul Imbeau*, 2010 QCCA 1050.
decision dismissing an application for judicial review of a decision by the Alberta OIPC, the Alberta Court of Appeal held that license plate information is not “personal information”, stating that:

… it is not reasonable to expand the meaning of “about an individual” to include references to objects that might indirectly be affiliated or associated with individuals. Some identification numbers on objects may effectively identify individuals. Many, however, are not “about the individual” who owns or uses the object, they are “about the object”.326

Recently, distinguishing the majority’s decision in Leon’s Furniture, the BC Commissioner took the position that license plate numbers did qualify as personal information under the BC FIPPA327 in light of the Victoria Police Department’s reason for collecting them, which was “to gain access to recorded information about identifiable individuals”.328 Adopting Conrad J.A.’s dissenting opinion in Leon’s Furniture, the BC Privacy Commissioner stated that “a licence plate number is “merely a conduit” to personal information that is not publicly available.”329 The inconsistency resulting from the application of expansionist interpretive approaches (i.e., “broad literal” and “relative” interpretations) in these decisions has generated considerable debate and uncertainty over the definition of personal information and the types of information that organizations are permitted to collect, use, or disclose without the consent of the individual.

Uncertainty can arise in this context because the existing approaches to interpreting “personal information” are vague with respect to how organizations are to determine whether the individual in question is “identifiable”.330 Specifically, these approaches do not provide

327 Freedom of Information and Protection of Privacy Act, RSBC 1996, C 165 [BC FIPPA].
329 Ibid. at para 66.
330 Gratton, supra note 183 at 124.
sufficient guidance on whether the organization should take into account illegal means in determining “identifiability”; on what resources it should expend in doing so; and where correlation needs to be considered, on what additional information and what kind of correlation should be taken into account. First is the question of whether illegal means should be taken into account when determining whether certain information is personal. That is, for example, whether the organization in question should evaluate the information taking into account the “possibility” of a security breach, unauthorized disclosure, or other illegal act. The question that also arises is whether such an occurrence ought to be likely, or whether the mere possibility is enough to qualify, for example, strings of non-identifying numbers as personal data.\textsuperscript{331} As Gratton states, “[g]iven that there is always a possibility, either technical (security breach) or illegal (illegal transfer of information that may allow the identification of additional information), this question is extremely relevant.”\textsuperscript{332} Opinions on this question, however, are not unanimous\textsuperscript{333}, and the expansionist interpretations under Canadian DPLs provide little guidance in this regard.

The second important shortcoming of the existing approaches to interpreting “personal information” under Canadian DPLs that causes uncertainty is their lack of guidance on the lengths to which organizations are required to go in assessing identifiability. Under the federal and Alberta statutes, for example, an individual will be identifiable if there is a “serious possibility” that he or she could be identified through “the use of that information, alone or in combination with other available information.” In BC, the information must be “reasonably capable” of identifying a particular individual “either alone or when combined with information

\textsuperscript{331} Gratton, \textit{supra} note 6 at 117.
\textsuperscript{332} \textit{Ibid.}
\textsuperscript{333} \textit{Ibid.} at 117-119.
from other available sources.” In neither case, however, does the case law offer further guidance on what kind of efforts should be made by an organization to determine whether a “serious possibility” exists or whether the information is “reasonably capable” of identifying the individual. Similarly, no further guidance is offered on what measures the organization ought to take in assessing whether “other available information” or “information from other sources” exists and is accessible. Gratton has described the increasing importance of quantifying the requisite efforts and resources needed in this context as follows:

In the context of online services, this [may] mean that the traceability of any information back to an individual can qualify that information as personal, even if the entity processing that information does not actually know the identity of the data subject. No distinction is made between information that can easily be linked to an individual and information that can only be linked with extraordinary means or with the cooperation of third parties.

Under this interpretation, every organization doing business on the Internet collecting or using … new types of data would have to be sure that there is no conceivable method, however unlikely in reality, by which the identity of individuals could be established. This may be a highly impractical approach, usually requiring considerable resources to implement. …

In a time where it is often possible, with a lot of resources and sophisticated technologies, to link certain data to an individual, additional guidance is necessary in order to determine how the notion of “identifiable” should be interpreted in the context of the Internet and new technologies.334

The expansionist interpretations of personal information under Canadian DPLs do not fill this gap and what results once again is a level of legal uncertainty that is difficult to justify.

Organizations are to left to ask, as do Lundevall-Unger and Tranvik, “[s]hould sophisticated, cutting-edge and expensive means be included, or only off-the-shelf and inexpensive tools and methods (like cookies or super-cookies)?”335

334 Ibid. at 123-124 [emphasis in original; footnotes omitted].
Third, the existing expansionist interpretations under Canadian DPLs require that correlation be considered, but do not provide more specific guidance on what additional information and what kind of correlation should be taken into account. For example, take the \textit{Schindler Elevator} decision, which suggests that “identifying an individual” means “distinguishing a particular individual”, but does not expressly provide guidance on what factors need to be taken into account in making such a determination (\textit{e.g.}, whether the information can be linked to “a name and a face”). In \textit{Schindler Elevator} and the cases that followed it, the BC OIPC found that information collected by GPS technology installed on company assets (vehicles and cellular phones) assigned to specific employees amounted to “personal information”. Therefore, we can assume that the employers in those cases could link a name and maybe a face to the individuals in relation to whom the information was being collected. As a result, although not free from doubt, it can be implied that information will be capable of “identifying” or “distinguishing an individual” under the \textit{BC PIPA} where it can be linked to identifiers such as a name and/or a face, but what other distinguishing factors will be sufficient remains uncertain.

Importantly, legal uncertainty is problematic for organizations in the private sector that manage personal information because if they do not know whether the data that they are handling constitute personal information, they cannot know whether they must comply with the obligations set out in the applicable DPL. Gratton describes the following examples of undesirable consequences of such uncertainty:

\begin{quote}
Organizations will not know whether they should be incurring costs to comply with [the DPL] (by investing in appropriate security measures to protect the data managed, \textit{etc.}) since they will not know whether their activities are governed by [the DPL]. In the event that they are to comply with the … DPL, this implies certain obligations for an
\end{quote}
organization managing the data such as providing a privacy policy (disclosing their privacy practices)\textsuperscript{336} pertaining to the collection and use of … new types of data, and obtaining consent from individuals.\textsuperscript{337} They may also have to grant access\textsuperscript{338} to the data to the individuals requesting it.\textsuperscript{339}

In addition, organizations have certain retention and destruction duties in defined circumstances (\emph{i.e.}, when the information is no longer necessary for the purpose for which it was collected)\textsuperscript{340}, so they need to know at what point they must destroy the information in compliance with these obligations. Certainty is needed in this context so that actors are able to govern their conduct in compliance with the applicable law. As a result, the second Bennett Moses/Gratton factor also weighs against the existing approaches to interpreting personal information in the Canadian private sector.

\subsection*{3.2.3 Obsolescence}

With respect to the third and final consideration in the Bennett Moses/Gratton framework, the expansionist approaches taken in interpreting “personal information” under Canadian DPLs may be (or may soon become) obsolete because they are “justified, explicitly or implicitly, on the basis of a premise that no longer exists.”\textsuperscript{341} These approaches focus on the “identifiability” of an individual, and as Gratton argues, “it is debatable whether the notion of identity is still relevant in the context of the Internet”.\textsuperscript{342} She explains:

\begin{quote}
Behavioural advertising may often involve the collection of IP addresses and the processing of unique identifiers (through the use of cookies). The use of such devices
\end{quote}

\textsuperscript{336} See for example, \textit{BC PIPA}, \textit{supra} note 23, s 5.
\textsuperscript{337} See for example, \textit{Ibid.} ss 6-9.
\textsuperscript{338} See for example, \textit{Ibid.} s 23.
\textsuperscript{339} Gratton, \textit{supra} note 6 at 116-117. [original footnotes omitted; new footnotes added]
\textsuperscript{340} See for example, \textit{BC PIPA}, \textit{supra} note 23, s 35.
\textsuperscript{341} Bennett Moses, \textit{supra} note 286 at 138.
\textsuperscript{342} Gratton, \textit{supra} note 6 at 138.
with a unique identifier allows the tracking of users of a specific computer even when
dynamic IP addresses are used. In other words, such devices enable data subjects to be
targeted or “singled out”, even if their real names or contact information are not
necessarily known. Similar concerns can arise in the offline world, using location data or
[Radio Frequency Identification] technology to profile individuals. New technologies
make it possible to identify the behaviour of a machine (device, computer) and the
behaviour of the individual behind the machine. It may therefore be possible to recreate
the personality of an individual in order to make certain decisions about the profile (and
thus the individual behind the anonymous profile) without needing the individual’s
identity (name and address). For example, an online business or merchant could refuse to
provide services to a certain online profile (even if there is no name attached to the
profile) because the profile information suggests that the individual behind the profile is a
pro-consumer activist. An insurance company could refuse to provide health coverage (or
to answer questions from a web visitor pertaining to the insurer’s health coverage
services) to an individual visiting its website for the main reason that the profile
information suggests that this individual has viewed websites for individuals afflicted
with certain diseases, even if the insurance company does not have the identity of the
individual, and regardless of whether its assumption is in fact accurate. …

The potential result is that the information being used to harm an individual (against which DPLs
aim to protect) is not captured by the interpretation of personal information under the DPL in
question due to its outdated “identifiability” requirement.

Similarly, as Omer Tene writes, definitions of personal data centering on the identifiability of an
individual are “outmoded not only in [their] perception of de-identification but also in [their]
view of personal data as a static concept” in that they fail to account for “the fact that data that
are ostensibly not about “an individual,” such as metadata, social grid analysis, or stylometry
(analysis of writing style), may have unambiguous privacy impact.” On the point of de-
identification, many authors have written about the “myth of anonymization”. In an influential
article in 2010, Paul Ohm warned that "[r]e-identification science disrupts the privacy policy

______________

343 Ibid. at 139-140 [citations omitted].
344 Tene, supra note 9 at 1242-1243.
landscape by undermining the faith that we have placed in anonymization.”³⁴⁵ Ohm contended that by collecting ostensibly de-identified pieces of information and connecting them to additional information available to them, adversaries are able to incrementally create a “database of ruin”, “chewing away bit by byte on individuals’ privacy until their profiles are completely revealed.”³⁴⁶ The examples Ohm and Omer use to illustrate this possibility include Latanya Sweeny’s American case study in 1999, in which Sweeney showed that 87% of the US population could be identified using just three innocuous data items: zip code, birthdate, and gender; doing so provocatively, by revealing the health records of William Weld, then governor of Massachusetts.³⁴⁷ In another example, University of Texas researchers Arvind Narayanan and Vitaly Shmatikov re-identified anonymized movie recommendations made available as part of the “Netflix challenge” by matching the de-identified database with another data resource that was available online.³⁴⁸ Other examples of “re-identification attacks” include on Amazon’s collaborative filter mechanism (i.e., “Customers Who Bought This Item Also Bought…”), in which researchers developed algorithms that take a moderate amount of auxiliary information about a customer and infer this customer’s transactions, showing that their attacks can be carried out by any Internet user, and that it is impossible to scrub data to prevent its re-identification in a foolproof way without also sacrificing its utility.³⁴⁹ As Ohm and Tene contend, in light of technological advances, “data are either robustly de-identified or useful, but not both.”³⁵⁰ Accordingly, if the notion of “identifiability” underlying the expansionist interpretations is not

³⁴⁵ Ohm, supra note 10 at 1704.
³⁴⁶ Tene, supra note 9 at 1240.
³⁴⁷ Sweeney, supra note 12.
³⁵⁰ Tene, supra note 9 at 1240; Ohm, supra note 10 at 1704.
already obsolete, it is reasonable to predict that its obsolescence is foreseeable as technology continues to develop at an unprecedented rate.

3.2.4 Summary
As a result, when examined in the context of this discussion, the three factors from the Bennett Moses/Gratton framework weigh in favour of adopting a new approach to interpreting “personal information” under Canadian DPLs. Over time, particularly in the face of rapidly evolving technologies, existing expansionist interpretations have become progressively unworkable, and are no longer adequate to further the fundamental objective of these laws. Specifically, the over- and under-inclusiveness and legal uncertainty that result from, as well as the impending obsolescence of, the existing approaches demonstrate that a different approach is justified. The question is: what approach would be preferable? In an effort to elucidate the answer to this question, below I review the leading approaches proposed by scholars in the field before suggesting that a more flexible purposive risk of harm approach, as proposed by Éloïse Gratton, might overcome the difficulties identified with the current approaches and as a result better promote the fundamental goal of Canadian DPLs to protect individuals against the risk of information-based harm while facilitating the free flow of information necessary for trade and commerce.
Chapter 4: Recommending a Purposive Risk of Harm Approach to Interpreting “Personal Information” under Canadian DPLs

In the previous chapters, I have outlined the key features and development of Canadian DPLs to show that their underlying purpose is to protect individuals against the risk of harm posed by the collection, use and disclosure of their personal information. I have also identified significant inadequacies with the expansionist approaches currently used under these statutes to interpret the definition of “personal information” thereunder. In this chapter, I outline key proposals advanced for new ways of identifying information that should fall within the scope of data protection laws in Europe, the US, and Canada. I then argue that the purposive risk of harm framework promoted by Canadian privacy scholar Éloïse Gratton would overcome the difficulties identified with the current approaches under Canadian DPLs and as a result better promote the ultimate goal of these statutes to protect only information that poses a risk of information-based harm.

4.1 Proposed Approaches to Identifying Information Subject to Data Protection Laws

In light of the inadequacies of existing approaches to defining “personal information”, numerous commentators promote the adoption of new ways of identifying what information should fall within the scope of data protection laws worldwide. Below I outline key proposals advanced in relation to DPLs in Europe, the US, and Canada. In general, these have fallen into two camps: one promotes abandoning the concept of “personally identifiable information” (PII) altogether while the other advances a modified PII approach. Recently, however, Gratton has proposed a framework that falls somewhere in the between these two camps. She does not support abandoning the concept of PII altogether but she promotes moving away from a focus on “identifiability” and focuses on the risk of harm instead.
4.1.1 Abandoning PII

Scholars such as Paul Ohm and Yuen Yi Chung argue that adequately protecting privacy requires abandoning the concept of PII altogether, as explained below.

4.1.1.1 Paul Ohm

Paul Ohm contends that the concept of PII is nonviable and irreparable. In the context of highlighting the problem of new means for re-identification of data, he writes that, "[n]o matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered."\(^{351}\) In Ohm’s view, “[t]he list of potential PII categories will never stop growing until it includes everything”, and the attempt to delineate PII is as ineffectual as the classic “whack-a-mole” carnival game.\(^{352}\) He explains: “As soon as you whack one mole, another will pop right up.”\(^{353}\) Ohm proposes that, instead of using the concept of PII, regulators ought to “prevent privacy harm by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security.”\(^{354}\) Accordingly, he promotes substituting our use of PII as a gatekeeper for privacy protection for a cost-benefit analysis applied to all data collection and data processing of any kind.\(^{355}\) Ohm argues that regulators “should weigh the benefits of

\(^{351}\) Ohm, supra note 10 at 1742.
\(^{352}\) Ibid.
\(^{353}\) Ibid.
\(^{354}\) Ibid. at 1706.
\(^{355}\) Ibid. at 1768-1769.
unfettered information flow against its costs and must calibrate new laws to impose burdens only when they outweigh the harms the laws help avoid.”

4.1.1.2 Yuen Yi Chung

Yuen Yi Chung agrees with Ohm that regulators should abandon the concept of PII because drawing on the distinctions between PII and non-PII is a sectorial approach that no longer guarantees any meaningful privacy protection. Chung, however, contends that the solution lies in relying instead on a “contextual continuum of reasonable expectations”. Drawing from Helen Nissenbaum’s concept of “contextual integrity”, Chung states that privacy norms are rooted in the details of societal, cultural and political expectations. Accordingly, the Chung’s proposed scheme begins with specific regulations around how one would reasonably expect data to be collected, stored, distributed and used in the context the information was collected. If the collection, storage, distribution or use of data fell outside of this reasonable expectation, it would automatically trigger a universal privacy protection, pursuant to which parties that violate this reasonable expectation are required to give clear and explicit disclosure and obtain informed consent. Relying on the work of Ohm and the Article 29 Working Group, Chung argues that in making specific regulations under given contexts, regulators must weigh different factors that serve as indicators of risk and instruments for reducing risk. These factors include motive and purpose, data-handling techniques, private versus public release, sensitivity and quantity. Chung writes that, “[i]f the risk is very high, regulators should feel obligated to create more

356 Ibid. at 1736.
357 Chung, supra note 166.
358 Ibid. at 441. Chung explains that contextual integrity “builds on the idea that almost everything - events, transactions and human behaviors - happen in a context.”
359 Ibid. at 441.
360 Ibid. at 442.
specific and restrictive regulations around the collection and use of information under specific circumstances”. The author points out that, “[w]hat is necessary to safeguard health records may not be necessary for online search inquiries”.  

Chung also posits that regulating information collection and usage on a contextual expectation requires an examination of contextual norms since contexts are largely made up of norms that define essential elements such as expectations, behaviors, and boundaries. Drawing further from Nissenbaum’s work, Chung explains that two types of informational norms form the basis of contextual integrity in information privacy: norms of appropriateness and norms of flow (also known as norms of distribution). Norms of appropriateness demarcate the type and nature of information about a person that is permitted and even expected to be revealed under specific circumstances. The example Chung uses here is that “a patient is expected to share her medical history and condition with her physician under a medical context, but not with her employer under a different context.” Thus, “norms of appropriateness protect the varying degrees of knowledge concerning different relationships with different people.” The other informational norms which form the basis of contextual integrity in information privacy are norms of flow, which govern the transfer of information from one party to another. Chung posits that “[i]nformation distribution equality can only be upheld with the information

361 Ibid.  
362 Ibid. at 441-442.  
363 Ibid. at 442.  
364 Helen Nissenbaum, “Privacy as Contextual Integrity” (2004) 79 Wash Rev 119 at 138; Chung, supra note 166 at 442.  
365 Chung, supra note 166 at 442-443.  
366 Ibid. at 443.  
367 Nissenbaum, supra note 364 at 138; Chung, supra note 166 at 443.
provider's freedom of choice and discretion”, arguing that contextual integrity in information privacy is violated when either of the two foundational informational norms is violated.\(^{368}\)

As a result, in making laws regulating the collection and use of information, regulators ought to “envision the reasonable, appropriate information that one may expect to produce to a first party under a specific context, and whether the information distribution to a third party respects a reasonable standard of information flow.”\(^{369}\) Chung provides the following example relating to online behavioural targeting regulations:

For instance, when a person orders a dozen Fuji Apples on a grocery website, she may well expect to see Fuji Apples as the first option in the drop-down menu for her shopping convenience, but not to receive Fuji Apple phone advertisements or see pictures of Fuji apples on every webpage she visits. Similarly, a person can book a gay pride retreat to San Francisco on a travel website but remain private about her sexual preference at her home and workplace. Thus cookies used to save preferences on the use of the website or user location would fall under the reasonable expectation of collecting and using such information while revealing the age and gender of the traveler and the nature as well as destination of the trip to a third party for marketing purposes would not.\(^{370}\)

Under Chung’s proposed scheme, the parties whose collection, storage, distribution or use of data violated the contextual integrity in information privacy in this type of way would be obliged to obtain informed consent before collecting data.\(^{371}\) This would include not only first parties or first party domains that collect information and third parties that use this information, but also those that store information in massive databases.\(^{372}\) By contrast, parties that collect, store, distribute and use information within the reasonable expectation under the particular

---

\(^{368}\) Chung, supra note 166 at 443.

\(^{369}\) Ibid.

\(^{370}\) Ibid. at 443-444.

\(^{371}\) Ibid. at 444.

\(^{372}\) Ibid.
circumstances have no duty to comply with Chung’s general privacy regulation.\textsuperscript{373} Chung’s scheme thus gives people the power to share information selectively, determined by the trust and nature of their relationships.

\subsection*{4.1.2 Modifying PII}

In contrast to Ohm and Chung, scholars in this camp argue that, despite its flaws, the concept of PII should not be abandoned. Instead, they propose new modified frameworks incorporating or elaborating on existing conceptions of PII, as explained below.

\subsubsection*{4.1.2.1 Boštjan Berčič & Carlisle George}

In the context of the European Union, Boštjan Berčič and Carlisle George have argued that relational database design principles can be applied to identifying personal data under the \textit{EC Directive on Personal Data Protection}. In relational database theory, a record (structurally) consists of two parts: a unique record identifier and data related to it.\textsuperscript{374} Berčič and George contend that by using the concept of record identifiers from relational database theory, we can ascertain \textit{in concreto} when a specific record contains personal data and when it does not within the scope of a particular DPL.\textsuperscript{375} Berčič and George propose rules that use four categories of record identifiers for deciding whether a record should be considered personal data: i) explicit full identifiers; ii) implicit full identifiers; iii) explicit partial identifiers; and iv) implicit partial identifiers. A full identifier (explicit or implicit) defines an individual uniquely.

\begin{footnotes}
\footnotetext[373]{\textit{Ibid.} at 444-445.}
\footnotetext[374]{Berčič & Carlisle, \textit{supra} note 292 at 237.}
\footnotetext[375]{\textit{Ibid.}}
\end{footnotes}
An example of an implicit full identifier is a social insurance number (SIN); and an example of an explicit full identifier is: “name, surname and date of birth taken together (i.e., presuming that name and surname alone do not suffice to identify an individual uniquely, while in combination with date of birth they do)”.

There is usually more than one implicit full identifier for an individual (for example in addition to a SIN, a person has a personal health number). There are also many possible explicit full identifiers (e.g., name, surname and residence; or, if this does not suffice to identify an individual, name, surname, residence and date of birth). A partial identifier (explicit or implicit), however, does not identify an individual uniquely, and must be supplemented with other (full or partial) identifiers in order to become a full identifier that gives rise to unique identification.

An example of an implicit partial identifier is the first set of three digits of a SIN, which typically identifies the province in which it was registered, but not an individual person. This partial identifier can be changed to a full identifier by, for example, adding other ciphers of SIN.

A name and a surname form an example of an explicit partial identifier, and changes to a full identifier if one adds to it date of birth or residence or both.

Berčič and George argue that using these four types of identifiers would be a desirable, that is, more certain, way to identify personal data under the EC Directive on Personal Data Protection. They propose the following rules. First, since explicit full identifiers (e.g., name, surname, date of birth) most certainly define an individual, everything communicated about this individual (e.g., where he lives, who he is married to, what kind of a car he drives) in a record with this type...
of identifier can most certainly be considered personal data. Second, “records identified with full but implicit identifiers such that one needs to obtain additional data (possibly kept in non-publicly accessible registers) in order to fully identify an individual, should [also] be deemed to fall within the category of personal data.”

By contrast, since records with partial identifiers do not define individuals uniquely, a partial explicit identifier (e.g., name and surname that together denote a multitude of individuals and that considerably narrow down the set of all individuals to those with the same name and surname but that still do not define one individual uniquely) together with data related to it (e.g., an individual’s salary) should not in general be considered personal data. This general rule is subject to exceptions, such as where the identifier, coupled with the data relating to it, results in unique identification. Similarly, with respect to implicit partial identifiers (for example the first few digits of SIN), if this type of identifier together with data related to it identifies an individual uniquely, then it should be considered personal data, and not otherwise. In summary, personal data are all data that relate to individuals that are fully identified (explicitly or implicitly), but not data that relate to individuals that are identified only partially.

Berčič and George also discuss whether an identifier by itself can be personal data, and whether personal data can be its own identifier. The authors contend that, “although it usually takes two elements to constitute personal data, it is also possible that only one element satisfies both

---

381 Ibid.
382 Ibid. at 241-242.
383 Ibid.
384 Ibid. at 243.
requirements and that for the record to constitute personal data, in extreme cases, only a singular element will suffice."\textsuperscript{385} The identifier alone can constitute personal data if it contains data about an identifiable individual, for example, where an identifier not only identifies an individual uniquely, but also conveys some information, such as the individual's age and sex.

Similarly, one or more items of data about an individual (\textit{e.g.}, name, surname, date of birth, residence, salary) “can identify this individual uniquely even if the data do not necessarily include an implicit identifier”.\textsuperscript{386} Berčič and George say it is indisputable that such data are about a unique individual: “if from these items of data we can select a subset which uniquely identifies an individual (or a set of individuals), what we have at hand is precisely a unique identifier and we can argue that such a record contains the data and the identifier and is therefore personal data.”\textsuperscript{387} Examples of data combinations that tend to uniquely identify an individual in this way include i) name, surname and date of birth; and ii) name, surname, date of birth, residence.\textsuperscript{388} With respect to data records with two identifiers, the Berčič and George say that, “[i]f the second identifier is considered data (about an individual), then the record will contain both the identifier and the data related to it and it will be considered personal data whereas if the second identifier is considered an identifier only (and not data), then the record will contain two identifiers and no data and may therefore not be considered a personal data record.”\textsuperscript{389}

\textsuperscript{385} \textit{Ibid.} at 245
\textsuperscript{386} \textit{Ibid.} at 246.
\textsuperscript{387} \textit{Ibid.}
\textsuperscript{388} \textit{Ibid.}
\textsuperscript{389} \textit{Ibid.} at 247.
Based on the rules described above, Berčič and George propose the following, more precise, definition of “personal data” under the *EC Directive on Personal Data Protection*:

Personal data is any data that relate to a fully identified individual, whereby identification is achieved either by means of an explicit identification (which requires no further linking of data) or by means of an implicit identification (which requires further linking of implicit identifiers with their more readable explicit counterparts but which does not require further collection of data).  

They also propose the following more concise alternative:

Personal data is any combination of a unique (full) identifier of an individual and data related to it, whether this identifier is explicit or implicit.

Further, the Berčič and George propose that the following “decision tree” be applied when determining whether or not information falls within their definition of personal data:

First, a data record should contain both an identifier (ID) and data related to it. If one is not present (i.e. there is no identifier, whether implicit or explicit, or there is no data related to it) and if the missing part (identifier or data) cannot be inferred from the context … then there is no personal data. Data items related to unidentified individuals are not personal data and so are not identifiers by themselves.

On other hand, if:

- there is at least one ID item and at least one data item (comprising the cases where the identifier itself is data or where the data contains the identifier…) or

- there is ID only, but personal data related to it can be inferred from the context or there is data only, but ID related to it can be inferred from the context …, then the data record can contain personal data subject to some further conditions regarding the data and the identifier.

Regarding the ID part, these conditions are:

- the ID should be full and explicit (partial identifiers do not constitute personal data),

---

390 *Ibid.* at 244.

- if the ID is full but implicit, then the identification must be either likely or possible without disproportionate effort (otherwise it is not personal data).

Regarding the data part, these conditions are:

- there should be at least one data item related to the identifier (this data item can be another identifier so two juxtaposed identifiers are personal data…).

- data item related to the identifier can be anything at all (i.e. personal data in the broad sense, something is considered personal data as long as it can be brought in connection with specific individual, but it doesn't have to describe him personally, hence an individual's car number plate would therefore count as personal data…).\(^\text{392}\)

Thus, Berčič and George’s proposed framework centers on “identifiability”, elaborating on how identifiability ought to be determined.

\[\text{4.1.2.2 Patrick Lundeavall-Unger and Tommy Tranvik}\]

Also writing in the European context, Patrick Lundeavall-Unger and Tommy Tranvik propose what they describe as a practical method for deciding the legal status of IP addresses as personal data, which they suggest can be used more generally to evaluate the relationship between natural persons, identifiability and information.\(^\text{393}\) Their approach involves two consecutive steps: i) the legality test; and ii) the likely reasonable test. Under the first test, illegal means of linking “names and faces” to IP addresses are never taken into account when assessing whether or not IP addresses are personal data; and only legal methods of identification should form the basis of these decisions.\(^\text{394}\) Under the second, “likely reasonable”, test, once any “illegal means” have been excluded, the question of personal data is resolved by assessing the costs (e.g., money, money, money…).\(^\text{392}\)\(^\text{393}\)\(^\text{394}\)

\(^{392}\) Ibid. at 249-251.

\(^{393}\) Lundeavall-Unger & Tranvik, supra note 335.

\(^{394}\) Ibid. at 58.
expertise, etc.) associated with using legal methods of identification. If the costs of employing these methods are exceedingly high, then the likelihood of identifying who is using which IP address is low, and IP addresses are not personal data as a result. However, if the costs are more modest, then the chance of identifying individual Internet users increases, and we should therefore conclude that the IP addresses (or other information) in question are indeed personal data.

### 4.1.2.3 Paul M. Schwartz and Daniel J. Solove

US scholars Paul Schwartz and Daniel Solove argue that the concept of PII should not be abandoned, even though the current approaches to PII are flawed. They advance a new approach called “PII 2.0”, which is based upon a standard rather than a rule, and accounts for PII’s malleability. PII 2.0 distinguishes between information that relates to an “identified” individual and that which relates to an “identifiable” individual, and treats these two categories differently. They argue that each of these categories appears at a different point on a continuum of risk of identification and that the necessary legal protections should also generally be different for each of them as a result. PII 2.0, they say, permits tailored legal protections built around different levels of risk to individuals.

---

395 Ibid.
396 Ibid.
397 Ibid.
398 Schwartz & Solove, supra note 236.
399 Ibid. at 1817. This approach differs from the reductionist model, which protects only “identified data”, and from the expansionist model, which treats identified and identifiable date as equivalent.
400 Ibid.
401 Ibid.
Schwartz and Solove begin by defining PII 2.0 as a standard (an open-ended decision making yardstick), rather than a rule (a harder-edged decision making tool). In their view, opting for a reconceptualization of PII as a standard is desirable because standards “permit broad discretion and allow the decision maker to take into account relevant factors”. As a result, PII 2.0 will better equip us to deal with situations of rapid change (for example in connection with social and technological development), and the heterogeneous nature of the behaviour regulated by DPLs, as well as to identify the areas in which rules would be more useful for defining information as PII or non-PII. Accordingly, the authors posit that the best starting point for information privacy law is to conceive of PII as a standard.

Schwartz and Solove go on to outline the features of their new model, explaining that rather than functioning as a “hard on-off switch”, PII 2.0 allows for legal safeguards for both identified and identifiable information that permit tailored FIPs built around varying levels of risk to individuals. The PII 2.0 model places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. This spectrum is divided into three categories with fluctuating boundaries: (1) information about an identified individual; (2) information about an identifiable individual; and (3) information about a non-identifiable individual. These categories do not have hard boundaries and each is prescribed a different regime of regulation.

402 Ibid. at 1870.
403 Ibid. at 1871-1872.
404 Ibid. at 1877.
405 Ibid.
Under the first category, information refers to an *identified* person when it singles out a specific individual from others, that is, a person has been identified when her identity is ascertained.

Under the second category, and in the middle of the risk continuum, is information that relates to an *identifiable* individual, meaning that specific identification, while possible, is not a significantly probable event. In other words, “an individual is identifiable when there is some non-remote possibility of future identification”, and the risk level for information in the second PII 2.0 category is low to moderate as a result.\(^{406}\) The third category is situated at the other end of the risk continuum and comprises *non-identifiable* information, i.e., information that carries only a remote risk of identification, taking into account the means reasonably likely to be used for identification.\(^{407}\) The test for all of these categories is a contextual one, taking into account factors such as “the lifetime for which information is to be stored, the likelihood of future development of relevant technology, and parties’ incentives to link identifiable data to a specific person.”\(^{408}\)

Schwartz and Solove explain that there are certain instances where *identifiable* information should be treated like information referring to an *identified* person. Specifically, where there is a substantial risk of identification of an individual, the information in question should also be treated as relating to an identified person. In other words, “identifiable data should be shifted to the *identified* category when there is a significant probability that a party will make the linkage or linkages necessary to identify a person.”\(^{409}\) The authors posit that this subcategory is essential,

\(^{406}\) *Ibid.* at 1878.
\(^{408}\) *Ibid.*
\(^{409}\) *Ibid.*
and requires an assessment of the means of identification likely to be used by parties with current
or probable access to the information, as well as the additional data upon which they can draw.\footnote{Ibid.}

As mentioned above, each of the three PII 2.0 categories is treated differently and accorded
tailored FIPs based on the corresponding level of risk to individuals. Recall the internationally
recognized FIPs, which are: “(1) limits on information use; (2) limits on data collection, also
termed data minimization; (3) limits on disclosure of personal information; (4) collection and use
only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice,
access, and correction rights for the individual; (6) the creation of processing systems that the
concerned individual can know about and understand (transparent processing systems); and (7)
security for personal data.”\footnote{Ibid. at 1880.} Under the PII 2.0 model, when information relates to an identified
person, all of the FIPs should in general apply. However, since identifiable information
do not yet refer to a specific person and may never do so, Schwartz and Solove argue that it is
not appropriate to treat information in the second category as fully equivalent to identified
information. Specifically, they say full notice, access, and correction rights should \textit{not} be granted
to an affected individual simply because identifiable data about her are processed.\footnote{Ibid.}

Accordingly, the only FIPs that ought to be triggered in these circumstances are those concerning
data security, transparency, and data quality.

\begin{flushright}
\footnotesize
\textit{The authors explain: “For one thing, if the law created such interests, these obligations would decrease
rather than increase privacy by requiring that all such data be associated with a specific person. This connection
would be necessary in order to allow that individual to exercise her rights of notice, access, and correction. In this
fashion, the law would create a vicious circle that could transform identifiable data into identified data. Moreover,
limits on information use, data minimalization, and restrictions on information disclosure should not be applied
across the board to identifiable information. Such limits would be disproportionate to risks from data use and also
would cripple socially productive uses of analytics that do not raise significant risks of individual privacy harms.”}
\end{flushright}
Finally, although not explicitly addressed by Schwartz and Solove, non-identifiable information would not trigger any FIPs.

4.1.3 Éloïse Gratton’s Purposive Risk of Harm Approach

Canadian scholar, Éloïse Gratton agrees that the concept of PII should not be abandoned, but instead of focusing on the risk of identification, as do Schwartz and Solove, she proposes a framework focused on the risk of harm. She posits that the “ultimate purpose” behind the adoption of DPLs is to “protect individuals against the risk of harm that may result from the collection, use and disclosure of their information”.413 On this basis, she advances a new purposive risk of harm-based framework for interpreting the term “personal information” in DPLs, which she argues will best achieve this ultimate purpose by ensuring that only data intended to be covered by DPLs (i.e., only data that presents a risk of harm) will in fact be covered.414 She argues that because her proposed framework is a flexible and context-based approach, it would ensure that only data presenting a risk of harm to individuals was protected, while facilitating the free flow of data that does not present such a risk. In this way, Gratton’s proposed framework achieves “a level of generality that corresponds with the lawmakers’ highest-level goal.”415

Gratton’s purposive risk of harm framework is founded on two central theories. First, information-based harm that occurs with respect to data collection and disclosure is subjective in

413 Gratton, supra note 6. at xxvii.
414 Ibid.
415 Ibid.
nature; while harm is usually objective in nature when it occurs at the point the data is used. Second, information-based harm can materialize at different points in the data handling process. In certain cases, harm occurs at the point of collection, while in other cases, it occurs at the point where the data is used or even disclosed. A framework based on these theories, Gratton argues, will better achieve the ultimate goal of DPLs by protecting data only at the time a risk of harm arises, and “in light of the importance or extent of such a risk of harm”.

Below I detail the risk of harm framework proposed by Gratton, following which I argue that it would indeed be desirable to use the proposed framework in interpreting “personal information” in cases under Canadian DPLs, using examples from case law decided pursuant to these statutes under more traditional interpretations of “personal information”.

### 4.1.3.1 Subjective and Objective Harm

Recall from Section 2.4.2 Gratton’s two categories of information-based harm. The first category comprises harm that is subjective in nature, as it typically relates to an emotional or psychological type of harm. As explained in greater detail below, Gratton argues that subjective harm is the type of harm that typically arises at the point of collection and disclosure due to a “a feeling of being observed (or under surveillance).” By contrast, the second category of privacy harm comprises harm that is objective in nature, that is, it is “external to the person harmed.” Objective privacy harm entails “the forced or unanticipated use of

---

416 Ibid.
417 Gratton, supra note 183. at 159.
418 Ibid. at 160-161.
419 Ibid. at 187.
information about a person against that person.” Gratton identifies three types of objective harm. The first is financial harm, including theft and identity fraud. The second is “information inequality”, which denotes circumstances in which information is used to discriminate against an individual by, for example, removing a benefit, tarnishing his or her reputation, or denying his or her application for employment, credit, a mortgage or a loan, etc. In relation to this type of harm, Gratton highlights concerns about consumer profiling such as “adaptive pricing” or “dynamic pricing”. The third type of harm in this category is what Gratton calls “physical harm”, including stalking, rape, and murder. Accordingly, objective privacy harm intimates “a more tangible kind of harm”, and typically arises at the point of use, which I explain in more detail below.

4.1.3.2 Points and Risks of Harm

Drawing from Daniel Solove’s “taxonomy of privacy”, Gratton identifies four basic groups of activities that are potentially harmful to privacy: information collection, information processing, information dissemination, and invasion. She links the first three groups to the data-handling activities governed by DPLs, proposing that each group carries with it a distinct set of risks that DPLs were designed to address, as explained in greater detail below. On this basis, she argues that the assessment of whether or not data qualifies as personal information ought to be specific to the data-handling activity in question, proposing a different test for each stage. She thus advances a “decision tree” (set out in Appendix B) that she says is a more desirable framework for identifying “personal information”, that is, one which is more suitable for furthering the
fundamental purpose of DPLs to protect only information that poses a risk of information-based harm. I describe the elements of Gratton’s proposed framework below.

4.1.3.2.1 Subjective Harm at the Point of Collection

As discussed above in Chapter 2, the first data handling activity typically regulated by DPLs is the collection of personal information, which typically relates to “the activity or the means by which personal information is gathered or obtained.” Collection gives rise to a risk of subjective harm, that is, harm that is psychological in nature and that arises from a feeling of being observed or surveilled, as discussed above. However, Gratton points to the relatively low risk posed by collection per se:

Given the volume of personal information readily available today, we should be focusing on the type of harm which can take place through other data handling activities, namely the types of harm triggered by the use or the disclosure of personal information. As a matter of fact, if an organization collects personal information without ever actually "using" it (for instance to take a decision which will impact the individual) and adequately protects the information against any potential disclosure (or a disclosure of the information would not be harmful to the individual), then the risk of harm at the "collection" level is either minimal, or it should be regulated by tools other than DPLs.

Accordingly, Gratton argues that when data are collected, the analysis that should be conducted to determine whether the information collected is personal should center on whether it creates a risk of harm upon being disclosed (e.g., in the context of a security breach) or upon being used. Only if such a risk can be identified should the data qualify as personal information, with the result being that the obligations to notify an individual of collection and obtain his or

425 Gratton, supra note 183 at 160.
426 Ibid. at 161.
427 Ibid.
428 Ibid.
her consent arise only where the data creates a risk of harm at the point of “disclosure” or “use”.\footnote{Ibid.} 

\subsection*{4.1.3.2.2 Subjective Harm at the Point of Disclosure}

The second data-handling activity governed by DPLs is disclosure or dissemination of personal information. Solove has defined this to mean the release or transfer to others of the information by the data holder, such that the data moves further away from the control of the individual.\footnote{Solove, supra note 422 at 489.} Gratton describes this activity as “the giving of information, the making available of information, the exchange of information or the sharing of knowledge”, and includes in its scope making information “increasingly available” (i.e., where the information disclosed by a party is already available to a certain extent).\footnote{Gratton, supra note 183 at 162.} Drawing further from the work of Daniel Solove, Gratton states that the harm associated with disclosure is typically psychological and, therefore, also falls into the “subjective” category of privacy harm. Solove explains that the harm that can be inflicted at the disclosure or dissemination stage includes a sense of betrayal where trust is breached, and embarrassment and humiliation where deeply primordial attributes about a person are exposed. These attributes include grief, suffering, trauma, injury, nudity, sex, and waste eliminating bodily functions, the exposure of which transgresses the social practices we have developed to “conceal aspects of life that we find animal-like or disgusting”, and offends “concomitant norms of dignity and decorum.”\footnote{Solove, supra note 422 at 536-537.} The person subject to the exposure can experience “severe and
sometimes debilitating humiliation and loss of self-esteem” and thus be impeded from fully participating in society.\footnote{Ibid. at 537.}

Based on Solove’s characterization of harm arising from disclosure, Gratton argues that determining whether data qualifies as personal information at this data-handling stage should involve an assessment of whether the disclosure will create a \textit{risk of subjective harm} to the individual. That is, a risk of psychological harm involving a feeling of embarrassment or discomfort due to the disclosure itself.\footnote{Gratton, \textit{supra} note 183 at 207.} Further, since the \textit{risk of harm} upon disclosure is highly contextual and can be difficult to isolate, Gratton advises assessing “identifiability” at this stage in light of the overall sensitivity of the information in question and calibrating the assessment according to the level of risk associated with that sensitivity. Specifically, she suggests considering a) whether the information is “identifiable”, that is, whether it can be linked to a unique individual (the more identifiable to a unique individual, the higher the risk of harm), b) whether the information is “intimate” in nature\footnote{Ibid. at 164. Gratton explains that “intimate” information means inherently “sensitive” information such as “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”} (the more intimate, the higher the risk of harm), and c) the extent to which the information was and will be available to third parties or the public (the less available it was prior to the disclosure or the more available it may become post disclosure, the higher the risk of harm).\footnote{Ibid. at 162-163.} If the conclusion flowing from this analysis is that disclosure poses a very low risk of harm to the individual (\textit{e.g.}, the data is not “intimate” in nature, it cannot be linked to a unique individual or small group of people, and it is already widely or publicly “available”), then, Gratton argues, the information should not qualify as
personal information, and the disclosure of the data should fall outside of the scope of DPLs as a result.\textsuperscript{437}

Notably, on the question of “identifiability” (or the potential for linking information to a unique individual) in her analysis at the disclosure stage (outlined above), Gratton addresses three important issues that impact the assessment, namely, illegal means, efforts to identify and potential correlation. The first question asks whether the potential for illegal acts or security breaches should be taken into account when evaluating whether or not data is identifiable (i.e., whether the data holder ought to consider illegal means that might be used to link the information to a unique individual). Gratton takes the position that the extent to which means of this nature should form part of the assessment should be commensurate with the extent of the risk of subjective harm.\textsuperscript{438} For example, if the data to be disclosed is not “intimate” in nature and is widely “available”, such that the risk of harm is low, illegal means should not be taken into account. By contrast, if the information is “unavailable” and highly “intimate” and thereby poses a higher risk of harm if disclosed, then “one should be more reluctant to dismiss considering” illegal means in this context.\textsuperscript{439}

The second question asks what kind and level of costs, efforts and resources should be expended when assessing whether data is “identifiable”. Here, Gratton suggests that, “as the effort and costs increase, the less likely it is that information will qualify as personal, and as the “intimate” nature of the information and its non “availability” factors increase, the more likely it is that the

\textsuperscript{437} Ibid. at 208.
\textsuperscript{438} Ibid. at 168.
\textsuperscript{439} Ibid.
information will qualify as personal.” Re40 Relevant to the third issue is that trivial bits and pieces of very common information are rarely attributable to a unique individual until correlated with different pieces of data about him or her. As a result, correlation is a key factor in the framework advanced by Gratton: this approach requires an evaluation of the ease with which correlation can occur, along with the level of “intimacy” of the information and the extent to which it is already “available”.441

4.1.3.2.3 Objective Harm at the Point of Use
The third and final data-handling activity governed by DPLs and covered by Gratton’s framework is the use of personal information. At this stage, Gratton argues in favour of replacing the “identifiability” metric with the likelihood of objective harm. This is because the “identifiability” of the individual in question is much less relevant at this stage, since the concern here is whether the information might have a negative impact on him or her, regardless of whether the individual’s identity can be ascertained.442 Gratton maintains further that the “intimacy” and “availability” of the information are not relevant factors when assessing the risk of harm at the “use” level. As a result, the test she advances for assessing if data qualifies as personal information at the point of “use” is only whether the data being used is likely to have a negative impact on the individual.443 If there is no likely impact for the individual or the potential impact is positive, then Gratton maintains that the data should not qualify as “personal information” and it can be used without further restrictions, as it was not intended to be protected

440 Ibid. at 172.
441 Ibid. at 175.
442 Gratton, supra note 6, at 349.
443 Gratton, supra note 183, at 208.
by DPLs when viewed through the purposive paradigm.\footnote{Ibid.} If a likely negative impact is identified, that is, an objective harm such as a financial harm, physical harm or some type of discrimination (including “information inequality” such as adaptive pricing), then the information would qualify as “personal information”. Flowing from this determination would be an obligation to ensure that the information is “accurate” and “relevant” to the intended use.\footnote{Ibid.}

The more significant the objective harm is determined to be, the more crucial it is that the information used to make a decision be accurate and relevant.\footnote{Gratton, supra note 6 at 366-367.} If, however, the information is not accurate and relevant, then the data should simply not be used for the purpose intended. Under Gratton’s proposed framework, the fact that the information can or cannot identify a unique individual does not need to be taken into account at the use level.\footnote{Gratton, supra note 183.}

\subsection{Summary}

Gratton proposes a purposive risk of harm-based framework that can be recapitulated as follows. Information being collected should be considered personal information only if it might trigger a risk of harm upon being “disclosed” or “used” (the tests applicable to making this determination are those set out in relation to the points of disclosure and use, which follow). To determine whether information being disclosed qualifies as “personal information” under the applicable DPL, one must consider the extent to which subjective harm (e.g., feeling of humiliation or embarrassment) might arise as a result, based on the following three criteria: 1) whether the subject of the information is identifiable (the more likely the information can be linked to a

\footnotesize
\begin{itemize}
\item \footnote{Ibid.}
\item \footnote{Ibid.}
\item \footnote{Gratton, supra note 6 at 366-367.}
\item \footnote{Gratton, supra note 183.}
\end{itemize}
unique person, the higher the risk of subjective harm); 2) whether the information is of an “intimate nature” (the more intimate it is, the higher the risk of subjective harm); and (3) the extent to which the information is “available” (the less available it was pre-disclosure or the more available it will become post-disclosure, the higher the risk of subjective harm). To determine whether information being used qualifies as “personal information” under the applicable DPL, one must consider whether objective harm (e.g., discrimination, or financial or physical harm) is likely to arise as a result. If so, the information qualifies as personal information and the information holder must ensure it is a) accurate, and b) relevant, before using it. If the information does not meet these “data quality” and “relevancy” tests, it should not be used by the organization seeking to use it. If the information being used does not trigger a risk of objective harm, it does not qualify as “personal information” and can be used without restriction. In short, Gratton proposes a purposive risk of harm-based framework that distinguishes between the three data handling activities governed by DPLs (collection, use, and disclosure) and centers on the particular type of harm (subjective or objective) that arises at each stage. Going forward, I will therefore call the framework she proposes the “risk of harm” or “purposive risk of harm” framework.

Below, I discuss how the proposed framework can overcome the shortcomings identified in relation to the expansionist approaches currently being used to interpret “personal information” under Canadian DPLs.
4.2 Recommending a Purposive Risk of Harm Approach

In the preceding sections, I argued that the inadequacies of the existing expansionist approaches to interpreting “personal information” under Canadian DPLs justify a new approach, and I surveyed the leading proposed approaches advanced in Europe, the US and Canada as potential substitutes. For the reasons that follow, I argue that Gratton’s nuanced and more flexible risk of harm framework is the most desirable approach to adopt under Canada’s DPLs.

First, as many have argued before me, abandoning the concept of “personally identifiable information” as proposed by Ohm and Chung is problematic because of the concept’s crucial function, that is, delineating the boundaries of data protection legislation. This position has been taken by, for example, Schwartz and Solove, who contend that without some concept of PII, there would be no limits on the scope of privacy law. As they cogently argue:

> In a world overflowing with information, the law cannot possibly regulate all of it. Yet, without adequate boundaries on regulation, privacy rights would expand to protect a nearly infinite array of information, including practically every piece of statistical or demographic data. The law would encompass nearly every fact about human behavior, no matter how generalized.448

Further, as Tene points out, abolishing the concept of PII and treating all data as personal and subject to DPLs “would create perverse incentives for organizations to forgo de-identification altogether and therefore increase, not alleviate, privacy and data security risks.”449 In addition, without a jurisdictional trigger, data protection regimes would be unworkable: they are “difficult enough to comply with and enforce today, the framework may well be unmanageable if it extends to every piece of information.”450 Further difficulty would also arise with respect to

---

448 Schwartz & Solove, supra note 236 at 1866.
449 Tene, supra note 9 at 1242.
450 Ibid.
Ohm’s proposal to assess the costs and benefits of every collection and release of data because “all costs and benefits are rarely known in advance”. 451 Although Ohm suggests that when in doubt, the law should limit the release or even the creation of large data sets, such data sets, “play an important role in research, health care, data security, and the dissemination of knowledge generally.” 452 Indeed, as Jane Yakowitz has pointed out, this approach significantly undervalues the social utility of data sharing. 453 In addition, because identity and identifiability are still the central focus of the modified PII approaches proposed by scholars such as Berčič and George, and Schwartz and Solove, these frameworks may be vulnerable to the same type of difficulties outlined in the preceding sections in relation to the existing expansionist approaches currently used under Canadian DPLs. The concerns that would be particularly applicable are under-inclusiveness and obsolescence.

The purposive risk of harm approach, by contrast, promises to overcome these shortcomings, by shifting away from a central focus on identifiability to a primary focus on risk of harm. Adopting this framework would thus fall in line with Ohm’s recommendation that:

Regulators … shift away from thinking about regulation, privacy, and risk only from the point of view of the data, asking whether a particular field of data viewed in a vacuum is identifiable. Instead, regulators must ask a broader set of questions that help reveal the risk of reidentification and threat of harm. 454

Further, adopting a purposive approach (as similarly argued by Aharon Barak 455 in relation to statutory interpretation generally) would enable decision-makers to interpret the definition of “personal information” in Canadian DPLs more consistently, “while remaining sensitive to

451 Schwartz & Solove, supra note 236 at 1866.
452 Ibid.
454 Ohm, supra note 10 at 1761.
important differences.” It would also fall in line with Gautrais and Trudel’s view that legal interpretation should emphasize the global context of the law in question, as well as its purpose and the original intent of the lawmaker. As stated by Gratton:

The definition of “personal information” is a legal construct. An interpretation taking into account the ultimate purpose behind DPLs will do just that: consider the rationale for this definition and determine how to best apply this rationale to any technology or piece of data in light of new technologies and the reality of the Information Age.”

Gratton designed her risk of harm framework to do just that: to promote the achievement of the “ultimate goal” of DPLs to protect individuals against the risk of harm arising from the collection, use and disclosure of their personal information. This, together with the flexibility inherent in the proposed approach, would align with the Ontario Court of Appeal’s view that the term “personal information” should have “…a very elastic definition, and [it] should be interpreted in that fashion to give effect to the purpose of the Act.”

In addition, because the risk of harm framework is a context-based approach that focuses on substantive outcomes, it provides for flexibility and as a result may better promote the goals of data protection regimes. Privacy and information experts view flexibility as critical in this context. For example, Joel Reidenberg and Paul Schwartz write that “[t]he ability of information technology to combine and share data makes impossible any abstract, noncontextual evaluation

\[456\] Gratton, \textit{supra} note 6 at 157.
\[457\] \textit{Ibid.} at 157 citing Gautrais & Trudel, \textit{supra} note 302.
\[458\] Gratton, \textit{supra} note 6 at 158.
\[459\] \textit{Citi Cards Canada Inc. v Pleasance}, 2011 ONCA 3.
of the impact of disclosing a given piece of personal information.”  \textsuperscript{460} Similarly, Microsoft has commented as follows in relation to the \textit{EC Directive on Personal Data Protection}: 

A more nuanced, or context-based approach to application of some of the Directive’s provisions might also strengthen data protection. Both data subjects and data controllers might benefit from the application of greater or lesser protections to personal data depending on the context in which such data are used. \textsuperscript{461}

In addition, as Gratton argues, a contextual approach is better suited to matching the level of protection to the level of sensitivity of information:

Personal information can be more or less sensitive (in terms of being potentially harmful to individuals) depending on the context, and the current definition of “personal information” may ignore this. For example, the appearance of an individual’s name on a company intranet page has fewer privacy implications than the appearance of the same name on a “blacklist” related to credit ratings. … DPLs may not necessarily make a distinction in light of the sensitivity of data-handling activities and may put all personal information on the same level … without taking into account the context of their availability. \textsuperscript{462}

Bennett Moses also emphasizes the importance of flexibility:

Both common law and statutory rules can be interpreted either rigidly or flexibly with varying degrees of weight given to their underlying purposes. A judge applying a rule rigidly will enforce the rule without considering whether such application is in line with the rule's purposes, whereas a flexible judge will seek to preserve the rule's intended effect in spite of its wording. A judge adopting a purposive approach in dealing with cases involving new technologies is more likely to reach the result that would have been reached at the time of the rule's creation, had the future been foreseen. \textsuperscript{463}

A purposive approach will provide this kind of flexibility, and can thus provide for more optimal protection because data presenting no risk of harm will flow freely. \textsuperscript{464} Consequently, entities that

\textsuperscript{460} Joel Reidenberg \& Paul Schwartz, \textit{Data protection law and online services: regulatory responses} (Directorate General XV of the Commission of the European Communities, 1998) at 9.


\textsuperscript{462} Gratton, \textit{supra} note 6 at 181 [footnotes omitted].

\textsuperscript{463} Bennett Moses, \textit{supra} note 286 at 279-280 [footnotes omitted].

\textsuperscript{464} Gratton, \textit{supra} note 6 at 180.
handle information that presents no palpable risk would not need to incur undue costs or engage in needless undertakings. For example:

… the proposed approach may require various commercial entities (websites, search engines, ISPs, etc.) that collect, use and disclose these data to obtain consent prior to collecting or using the data **only if** such data can trigger a risk of harm to the individual. They will have to dedicate sufficient resources to protect the information against a security breach in light of the risk of harm that such disclosure of data may trigger.\textsuperscript{465}

As a result, through the application of a more flexible approach such as Gratton’s risk of harm framework, Canadian DPLs could be better equipped to realize the balance they seek to strike between the protection of personal information and the needs of business entities.

Importantly, the flexibility and focus on context featured in the proposed framework may be capable of overcoming the inadequacies associated with the expansionist approaches currently in use under Canadian DPLs. First, the proposed approach may diminish the problem of over-inclusiveness and under-inclusiveness by focussing on situations where there is a “tangible risk of harm” rather than focussing on the identifiability of the individual in question.\textsuperscript{466} As a result, I note here that the risk of harm approach is preferable to the “zone of privacy” approach taken under federal public sector freedom of information and privacy legislation in Canada. This privacy-based approach requires information to fall within an individual’s “zone of privacy” in order to constitute his or her “personal information”.

\textsuperscript{465} *Ibid.* at 180, n 660 [emphasis added].
\textsuperscript{466} *Ibid.* at 188 and 180.
In the leading case, *NAV Canada*[^467], the Federal Court of Appeal interpreted the term “personal information” under the federal *Privacy Act*[^468], which defines the term as “information about an identifiable individual that is recorded in any form”.[^469] The case arose from an access to information request under the federal *Access to Information Act*[^470] for recordings and transcripts of air traffic control communications connected to four aviation incidents that were the subject of investigations and reports by the Canadian Transportation Accident Investigation and Safety Board (the Transportation Safety Board). The records contained information about weather conditions, the status of the aircraft, and air traffic control communications (including comments made by controllers and pilots). The Transportation Safety Board denied access to these records on the basis of the “employee personal information” exemption under the *Privacy Act*.[^471]

On judicial review, the Federal Court ruled that the requested information was “about an identifiable individual”, since it would allow the identification of the aircraft, as well as the location and operating initials of the specific controller involved. The Federal Court of Appeal disagreed, allowing the appeal and ruling that “personal information” must “be understood as equivalent to information falling within the individuals’ right of privacy”.[^472] The Court reasoned that privacy “connotes concepts of intimacy, identity, dignity and integrity of the individual”.[^473] Under this definition of privacy, the impugned information was not “about” an individual

[^467]: *NAV Canada*, supra note 243.
[^468]: *Privacy Act*, supra note 13.
[^471]: Together, the federal *Access to Information Act* and *Privacy Act* govern the privacy and access to information practices of the federal government and the statutes “must be read together as a “seamless code”, following a “parallel interpretive model” that balances the competing values of access and privacy”: *Dagg*, supra note 243 at paras 45 and 55-57.
[^472]: *NAV Canada*, supra note 243 at para 44.
because “it did not match the concept of ‘privacy’ and the values that concept was meant to protect”, and therefore it was not “personal”.

Thus, the privacy-based approach in the *NAV Canada* line of cases is narrower than risk of harm approach since, as discussed in preceding sections, the notion of data protection is broader than the notion of privacy protection in the strict sense (as embodied in the first and second wave conceptions of privacy). Therefore, an approach aiming to address information-based risk of harm includes but is not limited to the concern for privacy, and is better suited to prevent or minimize issues of under-inclusiveness.

Second, Gratton’s risk of harm approach may also provide guidance where there is uncertainty relating to the qualification of certain information as it provides a nuanced and detailed multi-pronged test. As an illustration of this, recall the example of Amazon’s alleged practice of consumer profiling and adaptive pricing through the use of cookies. Applying the risk of harm framework, one might determine that this type of use of the consumer’s profile creates a risk of objective harm (*i.e.*, discriminatory pricing), in which case the data being used for this purpose would qualify as personal information, triggering all of the attendant obligations under the applicable statute. Notably, Gratton provides guidance on the three areas in relation to which the existing Canadian approaches fall short, namely, illegal means, efforts to identify, and potential correlation. The proposed framework addresses these questions where they are most relevant, that is, under the branch of the framework applicable at the disclosure stage. As

---

475 Gratton, *supra* note 6 at 194.
explained above, the extent to which illegal means should form part of the assessment should be commensurate with the extent of the risk of subjective harm. For example, if the data to be disclosed is not “intimate” in nature and is widely “available”, such that the risk of harm is low, illegal means should not be taken into account in this context. I argue that in this way, Gratton’s framework better accounts for the reality that illegal means may in fact be used to access personal information than does the approach proposed by Lundevall-Unger and Tranvik\textsuperscript{476}, under which illegal means are never taken into account when assessing whether or not the information in question is personal data.

With respect to what kind and level of resources should be expended when assessing whether data is identifiable, the following guideline applies: as the effort and costs increase, the less likely it is that information will qualify as personal.\textsuperscript{477} This part of Gratton’s proposed framework thus incorporates the proportionality principle embodied in Lundevall-Unger and Tranvik’s “likely reasonable” test. With respect to the issue of correlation, the proposed risk of harm framework requires an evaluation of the ease with which correlation between a piece of information and an individual can occur, along with the level of “intimacy” of the information and the extent to which it is already “available”.\textsuperscript{478}

Third, Gratton’s risk of harm approach also reduces the concern about obsolescence of the notion of identity in relation to cases where, for example, a profile does not identify a specific individual but is still used to harm him or her. Gratton explains:

\textsuperscript{476} Lundevall-Unger & Tranvik, supra note 335.
\textsuperscript{477} Gratton, supra note 183 at 172.
\textsuperscript{478} Ibid. at 175.
The proposed purposive interpretation will therefore also be useful in order to ensure that a certain profile is governed by the relevant DPL, for instance, if it is used to take (sic) a decision about an individual possibly leading to some type of negative impact (regardless of the fact that the organization doesn’t … know the identity behind the said profile).  

Based on these considerations, the risk of harm framework may best ensure the attainment of the objectives of Canada’s DPLs and, accordingly, may be a desirable substitute for the expansionist interpretations of “personal information” currently being applied thereunder. To illustrate how the proposed framework might accomplish this in practice, below I apply it to a sample of cases that used the existing expansionist approaches in Canada to decide whether new data types and data collected, used or disclosed through new technologies qualify as “personal information”.

4.2.1 Applying the Purposive Risk of Harm Framework to Existing Cases

In this section, I illustrate how Gratton’s risk of harm framework might in practice more effectively promote the function of “personal information” as the gatekeeper to the protection of Canadian DPLs in light of these statutes’ fundamental purpose to protect only data that poses a risk of information-based harm. I do this by applying the framework to a sample of cases in which Canadian privacy commissioners (or their delegates), and in one case an arbitrator, used the existing expansionist approaches to decide whether new types of data or data collected, used or disclosed through new technologies qualify as “personal information”. I focus on new data types and technologies that have been posing significant challenges for data protection regulators and causing significant concern and discussion in the field: global positioning systems, Internet protocol (IP) addresses, cookies, and unique device identifiers.  

479 Gratton, supra note 6 at 192.
480 For examples of discussions about the challenges related to these technologies, see Ibid.; Lundevall-Unger & Tranvik, supra note 335; Sookman, supra note 85; McIntyre, supra note 312; and Clarke, supra note 311.
4.2.1.1 GPS

Global positioning system (GPS) is a satellite and ground based radio navigation and locational system that enables the user to determine locations on the surface of the Earth with tremendous accuracy. Organizations may wish to collect, use and disclose this type of location information for various purposes, such as management of vehicle fleets, vehicle security, or employee monitoring. In a 2012 guidance document, the OPCC, BC OIPC and Alberta OIPC state that location information could be personal information as long as it is “information about an identifiable individual”. Complainants in cases brought under Canadian DPLs have typically argued that such location information constitutes personal information attracting data protection. In these cases, Canadian privacy commissioners have consistently applied the expansionist approaches under scrutiny in this paper to find that information collected through GPS qualifies as “personal information”. Below, I review the facts and outcomes in a number of cases dealing with location information before evaluating how expansionist interpretations of “personal information” therein give rise to the identified shortcomings of these existing approaches. I then discuss how the application of the proposed risk of harm approach would overcome these inadequacies.

In *PIPEDA Case Summary #2006-351*, the Assistant Commissioner of Canada investigated a complaint about an employer’s plan to install GPS units on company vehicles in order to track

---


483 *PIPEDA Case Summary #351*, supra note 252.
employees’ daily movements. The information collected included location, mileage, speed, start
and stop times, and off-shift parking location. The employer argued that since the GPS system
did not collect location information associated with a particular individual, the information it
collected related only to the employer’s vehicles, and was not “personal information” as a result.
The Assistant Commissioner disagreed, finding instead that because the information collected
could “be linked to specific employees driving the vehicles, they are identifiable even if they are
not identified at all times to all users of the system”.484 As a result, based on an expansionist
reading of PIPEDA’s definition, the information qualified as “personal information” thereunder.

The Commissioner reached the same result using an expansionist approach in PIPEDA Case
Summary #2009-011485. In that case, the complainant was a driver hired by a contractor to
provide transportation services to mobility-impaired residents on behalf of a municipality. He
complained that the city’s use of GPS and Mobile Data Terminal (MDT) on vehicles operated by
the contractor for service efficiency and client safety purposes amounted to improper collection
and use of his personal information. The Commissioner found that the GPS and MDT data
collected did indeed constitute personal information, however, the complaint failed on the basis
that the employees had given implied consent, and there was no evidence that the information
was used for employee management.

484 Ibid. at para 29.
In BC, the relative expansionist approach has been applied to reach the same result. In *Schindler Elevator*\(^{486}\), the BC Commissioner investigated a complaint brought by a group of employees who objected to their employer’s use of GPS to monitor company vehicles. The technology recorded data such as vehicle location and information about the manner in which the vehicle was being driven, generating reports only where the vehicle’s use deviated from accepted norms. *Schindler Elevator*’s reasons for collecting the information included managing productivity and hours of work, as well as ensuring employees were driving safely.

Using a newly articulated, relative interpretation of “personal information”, the BC Commissioner found that the information in question was indeed personal information since vehicles were assigned to only one employee at time, and the company maintained records of who was operating a given vehicle at given times. In addition, while it revealed details about the vehicle, it would also “say something about the employee driving it”, such as the quality of the employee’s driving.\(^{487}\) The Commissioner also found that the disputed information was “employee personal information” as defined in the *BC PIPA* since the employer’s reasons in using the monitoring technology were solely for legitimate, reasonable, business purposes.\(^{488}\)

The BC OIPC has applied the relative interpretation articulated in *Schindler Elevator* in subsequent cases under the *BC PIPA* involving vehicle and cellular monitoring technologies. The decision in *Thyssenkrupp Elevator (Canada) Ltd.*\(^{489}\) involved the same GPS technology used in

\(^{486}\) *Schindler Elevator*, *supra* note 240.
\(^{488}\) For the definition of “employee personal information” under the *BC PIPA*, see Section 2.1.5 of this paper.
\(^{489}\) *Order P13-02*, 2013 BCIPC 24.
Schindler Elevator, which the employer used to monitor vehicles assigned to its mechanics to use in performing their duties. The system collected data about the location of the vehicle and engine status data relating to the operation of the vehicle. Thyssenkrupp Elevator’s reasons for using the GPS technology were similar to those offered in Schindler Elevator, namely efficiency, vehicle maintenance, identifying and addressing unsafe driving habits, locating employees who were unaccounted for, tracking time at job sites, and locating lost or stolen vehicles. Like the employer in Schindler Elevator, Thyssenkrupp Elevator did not continuously monitor the data collected by the GPS system, which generated exception reports only where the vehicle’s use deviated from accepted norms.

Applying the relative Schindler Elevator approach, the Adjudicator concluded that the information collected qualified as personal information, since the company knew what mechanic was assigned to each vehicle, and was capable of determining the location of a mechanic's vehicle at a given time, or using the engine status information to, for example, determine whether the mechanic has been speeding or operating the vehicle outside of work hours. The company had on at least one occasion used the GPS system information to warn an employee for speeding. The information also qualified as “employee personal information”. However, the complaint failed because Thyssenkrupp’s collection and use of the data in question was reasonable for the purposes of establishing, managing, or terminating an employment relationship. Specifically, the company had a legitimate interest in ensuring that employees complied with applicable laws and policies when driving company vehicles, and in verifying their time reporting. Further, there was no evidence that the employer was using the information for any purpose other than to manage the employment relationship.
Finally, the BC OIPC applied the relative *Schindler Elevator* approach in *Kone Inc.*\(^{490}\) in determining that information collected using GPS enabled cellular phones also constituted personal information. The case involved Kone Inc.’s use of GPS technology embedded in the employer owned cellular telephones assigned to its mechanics. The system collected information about the location of employees at any given time, and the company used this information to verify time reporting and to operate its dispatching system. Information was collected only when employees manually set their phones to “on-duty” while on shift. The reasons the company offered for collecting and using the information were to ensure accurate client invoicing, act as a time clock for employees to verify employee attendance and payroll, to optimize client response times, and to quickly locate employees in the event of an accident or emergency. Similar to Thyssenkrupp and Schindler, Kone Inc. did not continuously monitor employees but used the GPS data to produce weekly accuracy reports comparing employees’ reported location against the location information collected. The employer was alerted and the information examined further only where a significant discrepancy was identified.

In this case, the Adjudicator also concluded that the information in question qualified as personal information. The company assigned phones to its mechanics, knew which phone each mechanic possessed, and attributed the resulting GPS information to the specific mechanic. Further, tracking individually identified employees was a major purpose of this technology. In fact, company management had questioned at least one employee based on the data collected from the employee’s phone. The company collected and used the information, in part, to confirm employee attendance and to otherwise manage relationships with its employees. The information

\(^{490}\) *Order P13-01*, 2013 BCIPC 23.
also qualified as “employee personal information”, but its collection and use were acceptable under the BC PIPA. The Adjudicator commented that by virtue of being collected through GPS embedded in a phone used by the complainant, the information in question was more sensitive than information collected via GPS on company vehicles.

In Québec, complaints about technologies collecting location information in similar contexts are typically brought under section 43 of the province’s Act to establish a legal framework for information technology\footnote{An act to establish a legal framework for information technology, CQLR, C C-11 [An act to establish a legal framework for information technology].}, which provides that “…a person may not be required to be connected to a device that allows the person’s whereabouts to be known.”\footnote{See for example, Union internationale des constructeurs d’ascenseurs, local 89 c Ascenseurs Kone, 2012 QCCS 913.} In general, the case law under this section distinguishes between tracking a car (which is permitted) and tracking a person, and places an emphasis on the fact that the use of the technology in question is necessary given the lack of other options.\footnote{Yosie Saint-Cyr, “Employer Monitoring Employees With GPS Tracking”, (21 April 2011), online: Slaw - Can Online Leg Mag <http://www.slaw.ca/2011/04/21/employer-monitoring-employees-with-gps-tracking/> (accessed 12 October 2015).} The Act does not define the term “personal information”.

In all of the federal decisions described above, the OPCC applied an expansionist literal approach to interpreting the definition of “personal information” under PIPEDA. In the BC cases, the OIPC applied a slightly modified expansionist approach, \textit{i.e.}, the relative approach, as described above in Section 3.1.2. Importantly, the data in question in every case qualified as personal information identifying an individual, even though it was arguably identifying a device or object. Accordingly, the application of expansionist approaches in this context has arguably
resulted in over-inclusiveness. Further, it has resulted in uncertainty and inconsistency similar to that illustrated above in Section 3.2.2 in relation to licence plate numbers. Specifically, the application of expansionist approaches to interpreting “about an identifiable individual” has already produced inconsistent outcomes in Canada in relation to location information, even within the same jurisdiction. In contrast to the BC Commissioner’s decisions in Schindler Elevator and Thyssenkrupp Elevator, the arbitrator in a union policy grievance in BC, involving technology similar to that in issue in the latter cases, found that the information collected was not “personal information” under the BC PIPA.\textsuperscript{494} Ultimately applying the “zone of privacy” approach, the arbitrator found that the only information being collected that was “personal” was the name of the employee. The remainder of the information, however, was not “personal information” because it related to vehicle operation, was “of a professional and non-personal nature”, and did not engage the individual employees’ right to privacy.

The interpretive inconsistency in these decisions has generated considerable debate and uncertainty over the definition of personal information and the types of information that organizations are permitted to collect, use, or disclose without consent of the individual. This is in large part because the expansionist application of the definition of personal information and the term “identifiable” in this context can lead to counterintuitive and unpredictable outcomes. I argue that because Gratton’s risk of harm framework moves away from a binary approach, in which information can either be linked to an “identifiable” individual or not, toward one that centers on a flexible and nuanced analysis that assesses the risk of harm, it is a more conceptually defensible approach, and one that could prevent or at least significantly minimize

\textsuperscript{494} Otis Canada Inc v International Union of Elevator Constructors, Local 1 (Telematics Device Grievance), [2010] BCCAAA No 121 (Steeves).

124
any similar interpretive inconsistencies in relation to new technologies. It would also minimize the potential for under and over-inclusiveness.

In this part, I demonstrate how the proposed risk of harm approach might achieve this in practice, using examples from the decisions summarized above in relation to location information. First, under the proposed framework, information being collected should be considered personal information only if a risk of harm would arise at the point of disclosure or use. Second, if the organization disclosed the information, and a risk of subjective harm arose as a result based on the risk of harm test, the disclosure would be governed by the DPL, and the organization would bear the attendant obligations as a result (e.g., providing notice, obtaining consent, etc.).\textsuperscript{495} However, there was no evidence in any of the location information cases suggesting that the information in question was being disclosed. As a result, the focus in this section is on use and whether objective harm arises.

Applying the third branch of the risk of harm analysis, where an organization uses location technology to track its vehicles strictly for fleet management purposes, the data used for this purpose triggers no impact on individuals and would not be considered “personal information” under the applicable DPL as a result.\textsuperscript{496} Similarly, information used only to track vehicles for security purposes would also be excluded from the scope of the statute because it would have no foreseeable impact on the individual either (in fact the impact might be positive if, for example,

\textsuperscript{495} Gratton, \textit{supra} note 6 at 410, n 987.

\textsuperscript{496} \textit{Ibid.} at 410.
it ensured the security of the driver).\textsuperscript{497} As a result, the application of the proposed framework to the “personal information” determination in PIPEDA Case Summary #2009-011 would lead to the opposite result. The Commissioner found expressly that the only purposes for which the organization used the location information in that case were service efficiency and client safety. There was no evidence that the information was used for employee management. Accordingly, applying the proposed framework would mean that the information did not qualify as personal information since its use posed no risk of objective harm to the contracted employee. Applying the risk of harm framework would thus overcome the over-inclusiveness evident in the original decision in which the location information was deemed to trigger the organization’s obligations under \textit{PIPEDA}.

I note that in at least a couple of cases, the Commissioner indicated that one of reasons for the organization’s use of the information was for the benefit of the employees, for example, to refute allegations about them\textsuperscript{498} or to quickly locate them in the event of an accident or emergency\textsuperscript{499}. Had this been the only use for which the information was used, then under the risk of harm framework, it would not qualify as personal information as its use posed no objective harm to the employees, but rather promised to have a positive impact on them. In reality, however, the remainder of the location information cases involved multiple uses, including uses giving rise to objective harm, as discussed below.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{497} \textit{Ibid.} at 410.
\item \textsuperscript{498} \textit{PIPEDA Case Summary} #351, supra note 252 at para 11.
\item \textsuperscript{499} \textit{Kone Inc.}, supra note 490 at para 10.
\end{itemize}
\end{footnotesize}
Under the proposed framework, using location information as a basis for employee evaluation and potential discipline, would pose a risk of objective harm, and the DPL would apply as a result. The organization would, accordingly, need to inform employees of the collection and use, obtain their consent to the same, and ensure that the information is accurate and relevant for the intended use. Employers subject to the BC PIPA or Alberta PIPA, however, would be exempted from the obligation to obtain employee consent in this context if the information qualified as “employee personal information” under those statutes, and the collection and use was reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the employee.

All of the remaining GPS information cases cited above involved multi-purposes, including ensuring safety and development, protecting and managing assets, improving efficiency and quality of service, ensuring accurate payroll and client invoicing. However, although the organizations in these cases did not continuously monitor employees, they acknowledged using location information as a basis for employee evaluation and potential discipline. Accordingly, applying the proposed framework, a risk of objective harm would be found to arise, and the GPS information would qualify as personal information. Although the Adjudicator in Kone Inc. commented that, since it was collected through cellular GPS technology, the information in question was more sensitive than information collected via GPS on company vehicles, this would not be a consideration in the risk of harm analysis since sensitivity of the information is relevant

500 Gratton, supra note 6 at 410.
501 Ibid. at 410.
502 BC PIPA, supra note 23, ss 13, 16; Alta PIPA, supra note 22, ss 15, 18.
503 PIPEDA Case Summary #351, supra note 252; Schindler Elevator, supra note 240; Thyssenkrupp Elevator, supra note 489; Kone Inc., supra note 490.
only under the second branch of the framework, that is, only where the information is being disclosed.

Although the final outcome in these cases on the question of “personal information” would be the same using the proposed framework as it was through the application of existing expansionist approaches, I argue it would be more conceptually coherent in light of the purpose of Canadian DPLs to protect only information that poses a risk of harm. Further, Gratton’s risk of harm framework could overcome the under-inclusiveness and uncertainty resulting from expansionism in this context. This becomes clear through applying the framework to the Otis Canada decision described above. That case involved technology and location information similar to that in issue in the subsequent cases, Schindler Elevator and Thyssenkrupp Elevator. The uses to which the organization put the information were also similar, including for employee management and potential discipline purposes. However, in contrast to the BC Privacy Commissioner’s determinations in Schindler Elevator and Thyssenkrupp Elevator, the arbitrator found that the information collected was not “personal information” under the BC PIPA. In Schindler Elevator, the BC Commissioner expressly distinguished the Otis Canada decision, remarking that the arbitrator had not in that case taken the “proper” interpretive approach in light of the object of the BC PIPA, which she framed as balancing the competing values of protecting personal information and permitting its use by organizations for purposes that are appropriate in the circumstances.505

504 Otis Canada Inc. v. International Union of Elevator Constructors, Local 1 (Telematics Device Grievance), supra note 494.
505 Schindler Elevator, supra note 240 at paras 73 and 75.
What results from the *Otis Canada* decision is uncertainty due to the inconsistency with the Privacy Commissioner’s decisions, and also under-inclusiveness since it exempts from the *BC PIPA*’s protection individuals who faced a risk of harm arising from the use of their personal information. These inadequacies, however, would be overcome through the application of the proposed risk of harm framework to this entire set of cases. Applying it to the *Otis Canada* decision would mean that the location information was indeed personal information since its use gave rise to a risk of objective harm to the employees (*e.g.*, potential discipline). It would also remove from the realm any GPS information used solely for asset security or fleet management such that an organization using the information for these “benign reasons” would not be subject to DPL obligations. Thus, this outcome would be consistent with the outcome in the Privacy Commissioner’s decisions, and it would remedy the under-inclusiveness identified immediately above. It would, as discussed above in Section 4.2, also overcome the concern about obsolescence of the concept of “identifiability”.

### 4.2.1.2 IP Addresses, Cookies, and Unique Device Identifiers

As discussed above in Section 3.2.2, computers use IP addresses to communicate with one another on the Internet or other networks. Each computer is assigned a unique (typically numerical) IP address, which can be used together with additional information from the Internet service provider (ISP) to identify a specific subscriber who is online at a particular time. The OPCC has taken the position that an IP address can be considered personal information under *PIPEDA* if it can be associated with an identifiable individual.
A cookie is a small piece of text that is placed on a computer when an individual visits a website.

The Canada Privacy Commissioner has provided a very useful description of cookies in PIPEDA Case Summary #2012-001, as follows:

Cookies were created so that information could be saved between visits to a website. They collect and store information about individuals based on their browsing patterns and information they provide to a site. Cookies record language preferences, for example, or let users avoid logging in each time they visit a site. Almost all of the most popular websites use them. Cookies can be very useful because, without them, individuals would have to enter certain bits of their personal information each time they visit their favourite sites.

First party cookies are cookies set by the website (the "first party") being visited (or a sub-domain of that website) and shared with the user (the "second party"). … Third party cookies are cookies typically placed by advertising companies that display advertisements on certain websites. When an individual visits a website that has an advertisement on it, a cookie may be passed from the advertising company (the "third party") to the individual's computer. When the individual revisits the same website, or another website that uses the same advertising company, the third party cookie can be read by the advertising company. If the cookie contains a unique identifier, then information about the individual's visits to different websites can be linked together. In this way, a detailed profile can be built up about the individual (or others using the same computer) and their browsing habits. This information can then be used to target advertising to the individual. 506

The OPCC takes the position that, since organizations use cookies to collect information on user and visitor web usage across the Internet, and this can be used to build profiles of individuals, the information being collected by tracking cookies may constitute personal information.507 Unique device identifiers (UDIDs) assigned to portable devices can also be used for tracking and profiling purposes. Concerns usually arise when a decision is made about a profile that may be harmful to the individual behind the profile. The objective under Gratton’s risk of harm framework, then, is to determine how a profile is in fact being used.508

507 Ibid. at para 283.
508 Gratton, supra note 6 at 406.
In the decisions that follow, the OPCC has applied (explicitly or implicitly) a literal expansionist approach to interpreting the definition of “personal information” under PIPEDA in the context of cases involving the use or disclosure of information relating to IP addresses, cookies, and UDIDs. What has resulted in a number of these cases is that the data in question qualified as information identifying an individual, even though its use did not necessarily pose a risk of harm to the individual in question. In others, the information did not qualify as such where a potential risk of harm did exist. Thus, these cases illustrate the potential over- and under-inclusiveness that can occur as a result of the inflexibility of expansionist approaches and its focus on the concept of “identifiability”, which appears to be increasingly obsolete. Below, I demonstrate how the proposed risk of harm approach might overcome these difficulties.

IP addresses or cookies may be used in a way that creates no impact (or a positive impact) for individuals: the information may be collected and used to improve user experience on the website, for instance, to remember what’s in the user’s shopping cart or to remember the language of preference. Under the proposed framework, the data in such situations should not be governed by DPLs, but this type of data has qualified as personal information under the expansionist interpretation in some existing decisions.

PIPEDA Report of Findings No. 2014-011 (Ganz Inc.) involved an investigation into the information handling practices of Ganz Inc. Ganz marketed Webkinz plush toys and operated a related website for children. Among other things, the Commissioner found that children using

\[\text{---}\]

\[509\] Ibid.
\[510\] Ibid.
the company’s website were not being tracked and profiled for the purposes of delivering targeted advertising to them. Instead, the company used first-party cookies for the purposes of administering and managing the Website. Examples of such uses included recording the appropriate language for the user, the identification of registered users, restricting advertising or serving country or provincial-specific advertising, frequency-capping of Ganz advertisements, and identifying users who had opted out of third-party advertisements. Third-party cookies placed on Webkinz were for statistical purposes such as frequency-capping and advertising campaign analytics, and also for the purpose of identifying Webkinz users so that their information could be “segregated” and blocked from further profiling or tracking for the purposes of serving targeted online behavioural advertising (OBA). The Commissioner’s tests did not find any direct evidence that cookies were being used to target Webkinz users to serve OBA objectives. The Commissioner concluded however that Ganz had not conducted sufficient due diligence to ensure that advertising networks and other third parties were not setting tracking cookies on users of the Website for such purposes.

The Commissioner in this case appeared to take for granted that the information in the cookie built profiles qualified as “personal information” as there was no express discussion on this question. He commented, however, that many of the third party cookies found “appeared to contain unique identifiers, e.g. data fields were labelled with a variation of an “ID” tag such as “ID”, “UID” and exchange_uid”. Under the risk of harm framework, however, the information collected and used through cookies in this case would not likely qualify as “personal information” since its use had either no impact on the user, or a positive one (e.g., to prevent

512 Ibid. at para 223.
targeted OBA). As a result, the proposed framework could curtail over-inclusiveness in such circumstances and remove this class of data from the DPL rubric.

The proposed approach would similarly do so with respect to the over-inclusive determination in PIPEDA Case Summary #2009-010 (Bell DPI) that information collected by Bell through deep packet inspection (DPI), including IP addresses, qualified as personal information. In that case, the Assistant Commissioner considered whether online tracking that uses DPI technology to allow an ISP to link a particular subscriber ID to a unique IP address was subject to PIPEDA. DPI is a tool used by ISPs to view information transmitted on the Internet (e.g., from e-mails, downloads, uploads, etc.) in order to manage the ISPs’ network traffic. Information is transmitted via the Internet using a protocol that breaks information into packets, routes that information to its destination and reassembles the information in the packets into the original content. The content (or “payload”) is the user-generated information (such as e-mail content) that is surrounded by several layers of control information to ensure proper handling and routing.

In this case, the complainant alleged that Bell Sympatico (Bell) used DPI technology during Internet transmissions to collect and use personal information from its customers without their consent. The complainant also claimed that this practice collected more personal information than was necessary to fulfill the company's stated purposes of ensuring network integrity and quality of service. The complainant alleged as well that Bell did not adequately inform its customers of its practices and policies concerning the collection of their personal information during Internet transmissions. The Assistant Commissioner found that the complaint was not

---

well-founded with regard to the two matters of consent and limiting collection, but well-founded with regard to the matter of openness.

Importantly, the Assistant Commissioner considered whether any information that Bell was collecting or using for the purposes of DPI could be considered personal information. She explained first that her investigation had established that, to manage network traffic, Bell's DPI devices as configured at the time, collected and used the following information relating to a given communication: i) IP addresses; ii) subscriber ID/user identifier pertaining to Bell customers; and iii) type of software application that is being used to transmit the packet. The investigation showed further that Bell assigned its subscribers a dynamic IP address when a subscriber of its Sympatico Internet service connected to the network. Bell indicated that it bound each dynamic IP address to an invariable “subscriber id” that could be traced back to an individual Sympatico subscriber. In this way, Bell could determine which Sympatico subscriber was associated with a dynamic IP address at a given time. Given that Bell could link its Sympatico subscribers, by virtue of their subscriber ID, with Internet activities (in this case, type of application being used) associated with their assigned IP addresses, the Assistant Commissioner found that IP addresses in that context were “personal information”. By contrast, since there was no evidence to suggest that Bell could link IP addresses not associated with Sympatico subscribers with an identifiable subscriber, Bell could not be said to be collecting or using personal information with respect to IP addresses belonging to non-Sympatico subscribers.

Applying the proposed risk of harm approach would yield a different outcome. Since either no harm or a positive impact would result on the individual in question, the information would not
qualify as personal information and the company’s obligations under the DPL would not be triggered as a result. After all, the Assistant Commissioner expressly stated that Bell used the information only for the purpose of managing network traffic to ensure network integrity and quality of service, and that Bell was not using it for anything other than its stated purpose. Thus, this example illustrates how the proposed framework would better facilitate the collection and use of information for legitimate business purposes where such use poses no risk of harm to the individuals that can be linked to the said information.

The proposed framework could similarly facilitate the legitimate business collection and use of data where no risk of harm exists by correcting over-inclusiveness in cases such as PIPEDA Case Summary #2011-006\textsuperscript{514} (Facebook). In that case, the complainant claimed that Facebook was using social plug-ins (i.e., buttons and boxes designed to display certain Facebook functionality on third-party websites,” such as the “Like” or “Recommend” icons) to share his personal information without his knowledge and consent. A Facebook user can access a social plug-in while logged onto Facebook to see personalized content in the social plug-in that highlights any activity that his or her friends may have initiated on that site, such as recommending a news article on a news website. The social plug-in acts as a portal to Facebook for the user, but it does not provide the third party site hosting the plug-in with any access to Facebook user data. The Commissioner found that the complaint was not well-founded as there was no evidence that Facebook was sharing personal information with other sites as alleged. Further, Facebook had provided adequate notice about its collection and use of plug-in practices.

\footnote{\textit{PIPEDA Case Summary #2011-006}, [2011] CPCSF No 6.}
On the question of “personal information”, the Commissioner explained that for every visitor to a website containing a social plug-in, whether the visitor was a Facebook user or not, Facebook collected certain information generated from the visitor’s visit to the third-party website in question, known as log-level “impression” data. Such information included the date and time a visitor visited the web page, the referrer URL, the visitor’s general geographic location, the visitor’s browser cookie ID, the IP address associated with the visitor’s computer, the browser and operating system being used by the visitor, and with respect to Facebook users logged-in to their account, their Facebook user ID. With respect to non Facebook members, or members logged-out of Facebook, there was no evidence to suggest that Facebook did, or had the capacity to, link the IP address it collected or used to an identifiable individual. In such cases, the IP address was not personal information as a result. However, with respect to Facebook users who were visiting sites with social plug-ins while logged-in to their accounts, Facebook collected that user’s Facebook user ID. The Commissioner found that since this information allowed Facebook to clearly identify an individual, it qualified as personal information. Likewise, all of the other “impression” data generated where a Facebook user who was logged-in visited a website with a social plug-in also constituted personal information under the Act.

The above is an over-inclusive result in light of PIPEDA’s fundamental purpose to protect against the risk of information-based harm, which the application of the risk of harm framework could correct. Specifically, the proposed test would remove from the realm of DPLs data being collected and used for “benign” business purposes, i.e., where no potential harm to an individual arises. It would thus serve the needs of business entities while ensuring that potentially harmful information is indeed protected. The information in question in the Facebook case was
“impression log data”, which includes the IP address for all individuals and the user ID for logged in Facebook members. Once collected, the information retrieved from Facebook’s web servers was aggregated and retained for 90 days. Facebook also reported that it “de-identified” the impression log data by stripping the user ID from the data within the first 30 days following its collection. It then used the impression log data in a de-identified form to create aggregated metrics. According to Facebook, the log-level data of non-Facebook members who visited a site with a social plug-in was in “non-identifiable format”. With respect to its use of the information, Facebook reported that it analyzes the aggregated log level data to determine how its plug-ins are working and to improve user experience. With respect to its disclosure practices, statistics derived from de-identified and aggregated log data may be shared with Facebook’s product partners. Such information may include, for example, bucketed demographic information on the type of users who interact with a certain plug-in on any given site. While actual log level data is deleted after 90 days, statistical information is kept longer. Based on this evidence, in contrast to the Commissioner’s determination, the information in question would not qualify as “personal information” under the proposed risk of harm approach, for the following reasons.

First, in relation to Facebook’s own use of the data, the evidence showed that such use was only for the purpose of analyzing the aggregated log level data to determine how its plug-ins are working and to improve user experience. As a result, there would be either no impact on the individual or the impact would be positive. Applying the proposed framework would mean that the data would not qualify as personal information as a result.
The second question under the risk of harm framework is whether Facebook’s disclosure to product partners of statistics derived from de-identified and aggregated log data gives rise to a risk of subjective harm (e.g., humiliation or embarrassment). The likely answer here would be that it does not, in light of Gratton’s three subjective harm criteria. First, it appears highly unlikely that the identity of an individual user could be ascertained in light of the fact that it comprises statistics derived from aggregated log data that has been de-identified. Second, although some of the raw “impression log data” might potentially be considered intimate (e.g., it might show a particular webpage visited, such as one advertising treatment for a particular illness), it would be difficult to argue that what the data actually disclosed was “intimate” and thus potentially harmful since it was statistical data derived from aggregated raw log data. Third, although the data did not appear to already be in circulation or available to Facebook’s product partners, on balance the risk of subjective harm is low when the third criterion is weighed against the first two. As result, in contrast to the Commissioner’s determination, the data being disclosed would not likely qualify as personal information and Facebook would not be obligated to meet PIPEDA’s disclosure requirements in relation to it, and would thus be exempt from liability under the Act. The distinction between members who were logged-in versus members logged-out or non Facebook members would be immaterial in this context. This case example further underscores how effectively the proposed risk of harm approach facilitates balancing the needs of business entities against the right of individuals to protect their personal information.

Further, using the proposed approach would restrict the application of PIPEDA to only situations in which personal information is actually being collected, used or disclosed. PIPEDA Case
Summary #2001-25 illustrates this point. The case involved a complaint against a broadcaster who had attempted, through its advertising server, to collect NETBIOS information on the complainant’s computer, without his consent. The complainant had a computer equipped with both a cable modem for Internet connection and a firewall designed to detect and block attempts at intrusion. Every time he tried to log onto the organization's Web site, his firewall detected, rejected, and reported on, an attempt by the broadcaster's advertising server to gain access to the NETBIOS information on his computer. A NETBIOS is a computer’s common or “friendly” name related to its IP address. If an IP address is traced, it allows access to information such as Web sites visited by the computer’s user or recent passwords used in obtaining access to secure accounts. The Commissioner’s summary investigation in this case states that the likelihood of tracing an IP address is small if the user has dial-up Internet access, but significantly greater if the user has a fixed Internet connection via a cable modem, as was the case with the complainant.

After conducting internal inquiries, the broadcaster confirmed that the complainant’s allegation was true. The broadcaster explained that the network administrator, on installing Microsoft Windows NT had neglected to deactivate certain features that come automatically with that program. These features, known as Internet Name Services, enable a server to collect the NETBIOS information of Web site users. Once informed that the features were on, the network administrator promptly turned them off. The complainant subsequently confirmed that his firewall no longer detected any attempts by the organization to obtain his NETBIOS information.

515 PIPEDA Case Summary #2001-25, supra note 250.
The Commissioner was satisfied that in some circumstances, notably the complainant’s, a NETBIOS might be used to obtain information traceable to an identifiable individual. He determined therefore that the information at issue was personal information for purposes of the Act.

Applying the proposed risk of harm approach could serve to curtail the over-inclusiveness resulting from these types of circumstances. The evidence in this case showed that the collection of NETBIOS information (information related to the IP address in question) was inadvertent, and suggested that the information was not being used for any purpose. The Commissioner concluded that the organization’s breach of applicable PIPEDA principles was accidental and considered the matter resolved after the organization turned off the features of its system that were automatically attempting to collect the information. By contrast, under the proposed approach, the NETBIOS information would not qualify as personal information at all since it was not even being used or disclosed by the organization. This would remedy the over-inclusiveness of the original decision.

In addition to remedying potential over-inclusiveness, the application of the proposed framework can correct potential under-inclusiveness. For example, in IS Provider516, the Assistant Commissioner determined that the originating IP address qualified as personal information but that the port address did not. In that case, the complainant alleged that his ISP was reading his outgoing e-mail messages and, as a result, was declining to route them if they were not destined to travel through the ISP’s mail servers. The complainant subscribed to the ISP’s high-speed

516 PIPEDA Case Summary #319, supra note 322 [IS Provider].
Internet service. He also subscribed to a web-centred company’s third-party e-mail service, which allowed individuals to send and receive e-mail messages from external mail accounts. The complainant was upset because he could not send e-mails without going through his ISP’s mail servers. The ISP was making its customers use its outgoing mail server because it had anti-spam measures in place, and it maintained that as a responsible network administrator it had to implement network security measures to protect its network and its users.

The complainant was concerned that in order to route outgoing mail through its mail servers, the ISP was inspecting and screening his outgoing e-mails without his consent. He stated that his ISP’s technical support staff told him that it was “snooping” into the Transmission Control Protocol (TCP) portion, that is the user portion, of a packet and when the specific field for the destination TCP Port was set to 25, the ISP blocked access to outside e-mail servers. He believed that the port information was indivisible from the rest of the packet; therefore, by reading the port address, he believed the ISP was reading the entire e-mail. The ISP indicated, however, that there was no inspection of the content of the packet, aside from the standard inspection of the source and destination IP address in order to make a routing decision, and the inspection of the source and destination TCP port addresses. Under the terms of service that the complainant agreed to as a residential high-speed customer, all e-mail had to be routed through the ISP’s mail servers.

The complaint failed on the basis that the ISP had in its terms of service agreement notified and obtained consent from the complainant with respect to its practice of collecting and reading IP addresses. There was no evidence to suggest that the ISP read the entire e-mail packet without
the complainant’s consent. Notably, the Assistant Commissioner stated that an IP address can be considered personal information under *PIPEDA* if it can be associated with an identifiable individual, but a port address is not personal information as it is not linked to an identifiable individual. In the complainant’s case, he was assigned a “dynamic IP address”, which means that it changed each time he logged on. This IP address was associated with the particular computer he was using. The ISP did not identify the user before he or she was allowed to send e-mail, but ensured that the user was directly connected to the ISP network and was therefore a customer of the ISP. For the purposes of this complaint, which involved the sending of e-mail by the complainant, the Assistant Commissioner accepted that the originating IP address identified the complainant and was therefore his personal information. A port address (which the ISP needed to know in order to deliver the message being sent), however, was not personal information, as it was not linked to an identifiable individual.

With respect to the originating address, applying the proposed risk of harm framework would likely result in the same outcome, since the organization was using the originating address to determine whether it would delete the complainant’s outgoing emails if it met certain criteria suggesting they contained spam (posing a risk of objective harm to the complainant). With respect to the destination portal, however, the proposed framework would provide for a more flexible and nuanced analysis that could address potential under-inclusiveness. The organization was also using the destination portal information to make determinations about rerouting or deleting the complainant’s outgoing emails if they appeared to contain spam. Depending on one’s perspective and prevalent social norms, deleting emails containing spam could either have a positive or negative impact on the potential recipient behind the portal address. It is likely that
such use of the destination address would be deemed to have a positive impact on the individual behind the destination portal, and thus the outcome using the proposed risk of harm framework would be the same as in the original decision and the information would not qualify as personal information. However, the proposed approach would provide the flexibility to decide otherwise where, for example, receiving spam, such as advertisement for discounts or sales, is determined to be objectively positive for the recipient and thus its deletion would result in a negative impact on the individual and trigger the protection of the DPL as a result.

Another example of potential under-inclusiveness that the risk of harm framework can remedy in this context arises in relation to the decision in PIPEDA Report of Findings No. 2015-001 (Bell RAP), which involved an investigation into Bell’s “Relevant Advertising Program” (RAP). As part of this program, Bell used customer profiles it created with its customers’ network usage information and account/demographic information to support targeted advertising. As explained in the decision, generally speaking, a Bell customer profile included demographic information and account information combined with network usage information, such as specific websites visited and apps used on a Bell customer’s mobile device. The customer profile also included interests Bell had inferred from such network usage. For instance, a customer profile could indicate that a Bell customer is an English-speaking female, between the ages of 26 and 30, in the city of Montreal, who has a medium to high interest in hockey and who recently visited www.cbc.ca/news. Also as part of the RAP, advertisers created, via a special web interface, “ad profiles” that defined the audience of Bell customers to whom they would like to deliver targeted ads (e.g., 26-30 year old males in the city of Ottawa with below average credit and an interest in

\[\text{IPEDA Report of Findings No 2015-001, [2015] CPCS No 1.}\]
rock concerts). Ad profiles were comprised of a number of “dimensions”, each corresponding to a specific type of information captured in Bell’s customer profiles. Finally, Bell facilitated the delivery of targeted ads by RAP advertisers to Bell customers by sending a temporary customer ID and customer profile identification number to the RAP advertiser. This would allow the advertiser to deliver a targeted ad to the Bell customer whose customer profile matches an active ad profile. The Commissioner noted that Bell did not deliver the ads directly, and did not share the identity of the Bell customer with RAP advertisers during the process. The OPCC ultimately concluded that Bell’s use of the information for the RAP was an appropriate purpose but decided that express opt-in consent was required because of the potential sensitivity of the browsing behaviour data being used under the program. In response to the decision, Bell withdrew its the program.

Notably, the OPCC in Bell RAP did not expressly analyze whether the temporary customer ID and customer profile identification numbers that Bell was sending to RAP advertisers qualified as “personal information” attracting the protection of PIPEDA. In fact, the OPCC found “no evidence that Bell [was] disclosing personal information to RAP Advertisers” even though it had reported earlier in the decision that Bell was sending temporary customer IDs and customer profile identification numbers to RAP advertisers, and then later in the report emphasized that a “risk persist[ed] that advertisers could link Ad Profile information to an identifiable individual.” I would argue that this is an under-inclusive result since subjective harm could arise from Bell’s sharing of customer IDs and profile ID numbers. By contrast, the application of

518 Ibid. at para 13.
519 Ibid.
Gratton’s subjective harm test would likely yield an outcome more in line with PIPEDA’s goal to protect individuals against such harm. This is because ad profile information could be linked to identifiable individuals, presumably through the temporary customer profile identification numbers advertisers received from Bell. Further, the information to which advertisers could gain access could be sensitive, including customers’ credit scores and online browsing habits. Finally, the information was not available to the advertisers prior to being disclosed as part of the RAP. Under such circumstances, the data could qualify as “personal information” under the risk of harm approach, and trigger Bell’s obligations under PIPEDA because the test focuses on harm to the customer and not the nature of the information as “identifiable” or not in the abstract.

These types of cases bring into focus the obsolescence of the concept of “identifiability” and the concern about re-identification in the context of rapidly evolving technologies and sophisticated understandings and uses of the same. As demonstrated above, Gratton’s shift away from an “identifiability”-centered and rigid approach would be a welcome and effective solution to these issues, as illustrated below in relation to the last case I examine in this paper, PIPEDA Report of Findings No. 2013-017 (Apple). In that case, the complainant alleged that Apple was using and sharing her personal information in the form of a unique device identifier (UDID) for tracking purposes without her knowledge and consent. Apple assigns a UDID to each iPhone, iPad and iPod Touch (iOS Devices) prior to sale. The company maintained that a UDID was not personal information because it alone could not be used to identify a user. However, the OPCC’s investigation revealed that Apple also had access to Apple ID account details for each iOS

Device user. As a result, the OPCC viewed UDID as personal information.

As explained in the decision, Apple used UDID for administrative and maintenance purposes. In that context, the OPCC did not consider UDID to be sensitive personal information and it was satisfied that Apple had adequately explained such practices via general explanations in its privacy policy. By contrast, the OPCC found that UDID was used by Apple, and disclosed to third party app developers, for the purpose of delivering targeted advertising to iOS Device users. In that context, the OPCC viewed UDID to be sensitive personal information as it could be used to create a detailed user profile, similar to a persistent cookie. While the OPCC concluded that Apple offered easily accessible opt-out options regarding the use of UDID in the delivery of targeted advertising, it found Apple’s explanations (which were comprised mainly of broad generalized statements in its privacy policy) to be insufficient. As a result, the OPCC recommended that Apple provide notice in a clear and prominent “just-in-time” way to shed proper light on the practice for users. Due to changes Apple made to its practices during the course of the OPCC’s investigation, the matter was found to be well-founded, but resolved.

In this case, the OPCC found that UDIDs qualified as “personal information” under the Act since Apple had the capacity to “link and associate” such identifiers with individual Apple account holders. The application of the risk of harm framework would likely yield the same outcome at present; however, it would leave open room for consideration of rapidly evolving technologies and social and legal norms and how these factors impact our notions of harm in this context.

__________________________

521 Ibid. at para 35.
First, the proposed framework would require assessing whether a risk of objective harm arises from Apple’s own use of UDIDs. No risk of objective harm would arise from Apple’s use of the data for the purposes of administration and maintenance, however, such risk might arise from its use of the information for the purpose of serving interest based ads.

The risk of harm approach thus leaves room for considering whether such harm arises in the circumstances. This flexibility is particularly important in the context of profiling and behavioural advertising since in the words of Gratton, “[t]he jury is still out on whether behavioural advertising practices are harmful to individuals.”522 Some say these practices are not particularly harmful since much information in this context is amassed and processed by computers, not humans, making these marketing practices less invasive and thus less harmful.523 In this vein, the Canada Commissioner in Bell RAP524 found that Bell’s purpose in using account/demographic and network usage information to deliver targeted ads to be appropriate in the circumstances of that case. Critics, however, point to concerns such as the associated threat to the consumer’s ability to control the flow of his or her own personal information.525 The flexibility proposed framework would allow for these types of debates to be taken into account so that the determination reached accords with the balance DPLs seek to strike between the protection of personal information and the needs of business entities.

522 Gratton, supra note 6 at 319.
523 Ibid. at 319.
524 Bell RAP, supra note 517.
525 Gratton, supra note 6 at 413, n 1007.
In any event, whether or not a risk of objective harm would be found using the proposed framework in this case, it is likely that a risk of subjective harm would be found, thus ensuring the data was protected under the Act where it was being disclosed to third parties. With respect to the framework’s first subjective harm criterion, individuals behind the UDIDs could easily be identified through their account information, including by illegal means and without excess effort or resources. Second, as stated by the OPCC in this case, UDIDs can constitute sensitive personal information since they “can be used in the compilation and construction of extensive user profiles”.

Third, there was no evidence to suggest that the information was available to the third parties or otherwise before being shared. As a result, disclosure would pose a risk of subjective harm in this case, so the information would qualify as “personal information” attracting the protection of PIPEDA.

4.2.2 Summary

On the basis of the foregoing, applying Gratton’s risk of harm framework to cases previously decided based on expansionist approaches to interpreting “personal information” further demonstrates the ways in which the proposed approach can overcome the shortcomings of these existing approaches. As a result, I argue that the proposed framework could indeed better ensure the attainment of the fundamental goal of Canadian DPLs to protect individuals against the risk of information-based harm while facilitating the free flow of information for business purposes.

---

526 Apple, supra note 520.
4.2.3 The Price of Flexibility in a Purposive Risk of Harm Approach

Although using the risk of harm framework is a more preferable approach for interpreting “personal information” under Canadian DPLs than are existing expansionist approaches, its flexibility does come at a price. First there is the difficulty inherent in determining whether a risk of “subjective harm” (e.g., humiliation or embarrassment) exists on behalf of the person who may be subject to said harm, and in accommodating the potential differences between the subjective views of individuals. In the context of legal proceedings resulting from privacy complaints, where the decision-maker or regulatory body has access to the testimony (and thus subjective views) of the individual(s) whose personal information was or is being collected or disclosed, the question of subjectivity likely poses little challenge. However, outside of that context, ascertaining subjective harm, and accommodating potentially conflicting subjective views, could foreseeably become a quagmire for organizations making this assessment.

In some cases, the answer would be obvious. For example, an organization contemplating disclosing UDIDs like Apple was found to have done in PIPEDA Report of Findings No. 2013-017527 could easily predict the subjective views of their customers. It would be absolutely clear that otherwise unavailable “extensive user profiles” that could easily be linked to an individual through their account information would fall within the definition of “personal information” under the proposed framework’s subjective harm rubric. Presumably no one would subjectively want their identity to be linked to sensitive information about them through illegal means or otherwise. In other cases, however, the answer would be less clear. For example, where the profiles in question are less extensive and contained information that is only “borderline”

527 Ibid.
intimate, where some of the more intimate information is already “available”, and where it is questionable whether the individuals behind the profile could be identified, through illegal means or otherwise. In such circumstances, the scale would not clearly tip in one direction or the other and indeed may vary from person to person.

Another similar issue could potentially arise for organizations under the proposed framework’s objective harm rubric. Specifically, the flexibility of the framework could foreseeably result in uncertainty for organizations determining whether the particular use they are contemplating could result in harm that is “objective” by Gratton’s standards, particularly in relation to practices that are new or controversial. This potential problem can be illustrated using OBA as an example. As explained in the preceding sections, the advantages of using the risk of harm framework in cases such as Bell RAP\(^{528}\) and Apple\(^{529}\) includes its allowance for taking into account prevailing soci
dal and legal norms and debates associated with profiling and behavioural advertising. An obvious problem arises, however, where these debates are not settled, or where there is no “official” or “majority” opinion, as is currently the case with OBA.

While the flexibility of the proposed framework can give rise to these types of challenges, they are not fatal to my central thesis for the following reasons. First, developing case law would provide some guidance to make clearer the circumstances in which information would qualify as “personal” under the framework. Organizations could rely on the genius of a growing body of jurisprudence that balances the interests at stake in real cases. The second, more persuasive,

---

\(^{528}\) *Bell RAP, supra* note 517.

\(^{529}\) *Apple, supra* note 520.
reason relates to a practical solution organizations could implement in the face of any attendant uncertainty: setting out in detailed and explicit terms the purpose(s) for their intended collection, use or disclosure when seeking consent from the user. Organizations, such as advertisers, would thus be encouraged to be more transparent about their personal information handling practices and the consent they obtain would be truly informed as a result.

Finally, with respect to determining objective harm, Gratton does provide guidance in this regard in that she identifies three types of objective harm arising from the use of personal information: i) financial harm, ii) physical harm, and iii) discrimination (including “information inequality” such as adaptive pricing). Therefore, with respect to OBA, for example, an organization would need to determine if the type of advertising they deliver could result in any of these harms. In most cases, physical harm would likely fall away, as would financial harm (which includes harms such as fraud and identity theft). The organization would be left to assess whether its OBA could result in “information inequality”, which would be unlikely unless it could point to some “tangible harm” such as adaptive pricing. This is particularly so in light of, for example, the Canada Privacy Commissioner’s decision in Bell RAP530 that Bell’s purpose in using account/demographic and network usage information to deliver targeted ads was an appropriate use under PIPEDA. Therefore, adopting the risk of harm framework could ensure in this context that only data-handling practices that pose a risk of “truly” objective harm are regulated by DPLs, while practices that do not pose such risk are left to be regulated by the market, where the consumer decides whether or not to be swayed by “benign” OBA.

530 Bell RAP, supra note 517.
Chapter 5: Conclusion

The unprecedented pace of technological and societal change continues to pose significant challenges for regulators and decision makers worldwide seeking to define “personal information” in order to delineate what type of information should fall within the scope of DPLs. Decision-makers assessing this question under Canada’s private sector DPLs have taken an expansionist approach, which I argue falls short in light of these statutes’ fundamental purpose: to facilitate the needs of private sector business entities to collect, use and disclose information while protecting individuals against information-based harm. As examined in Chapter 2, this fundamental purpose is evident from the historical development, purpose provisions, and key features of these statutes, as well as the body of jurisprudence in which these laws are analyzed.

Against this backdrop, the first main objective of this thesis has been to survey and critique existing approaches to interpreting the definition of “personal information” under Canada’s private sector DPLs in order to show that a different approach is justified in light of these statutes’ principal purpose. As outlined in Chapter 3, the PIPEDA, Alberta PIPA, and BC PIPA all define personal information as “information about an identifiable individual”. The DPL in Québec defines it as “any information which relates to a natural person and allows that person to be identified”. Accordingly, the statutory definitions of “personal information” in Canadian DPLs are identical or virtually identical, with the key element being “identification” or “identifiability”. Decision-makers interpreting the statutory definition of “personal information” under these laws have adopted “expansionist” approaches (i.e., “broad literal” and “relative” approaches) based on the concept of identifiability. This has meant that information qualifies as
“personal” if it has been linked to a particular person, or might be so linked in the future either directly or in combination with other information.

Building on the work of Gratton and Bennett Moses, I also argue in Chapter 3 that, due to rapidly evolving technologies, these existing approaches fall short in light of the DPLs’ fundamental purpose to protect only data that poses a risk of information-based harm, demonstrating that a different approach is justified as a result. Specifically, the over and under-inclusiveness and legal uncertainty that have resulted from, and are likely to continue resulting from, these approaches, as well as their impending obsolescence, frustrate the fundamental goal of Canadian DPLs, thus warranting a different approach.

The second objective of this thesis has therefore been to recommend a purposive risk of harm framework as a desirable alternative to existing expansionist approaches to the interpretation of the definition of “personal information” under Canadian DPLs. In Chapter 4, I conduct a review of the literature discussing the leading proposed approaches to identifying “personal information” in Europe, the US, and Canada. This includes a detailed overview of Gratton’s proposed purposive framework, which focuses on risk of harm and is founded on two central theories. The first is that information-based harm that occurs with respect to data collection and disclosure is subjective in nature; while harm is usually objective in nature when it occurs at the point the data is used. Second, information-based harm can materialize at different points in the data handling process. In certain cases, harm occurs at the point of collection, while in other cases, it occurs at the point where the data is used or even disclosed.
Gratton argues for a risk of harm-focused interpretive framework that distinguishes between the three data handling activities governed by DPLs (collection, use, and disclosure) and centers on the particular type of harm (subjective or objective) that arises at each stage. Under Gratton’s proposed framework, information being collected should be considered personal information only if it might trigger a risk of harm upon being “disclosed” or “used”. Information qualifies as “personal information” at the point of disclosure where such disclosure gives rise to a risk of subjective harm (e.g., humiliation or embarrassment), taking into account three factors: “identifiability”, “intimacy”, and “availability”. Information qualifies as “personal information” at the point of use, where such use poses a risk of objective harm (e.g., discrimination, or financial or physical harm). If such a risk arises, the information holder must ensure the personal information is accurate and relevant, before using it. If the information does not meet these “data quality” and “relevancy” tests, it should not be used. If the information being used does not trigger a risk of objective harm, it does not qualify as “personal information” and can be used without restriction.

In Chapter 4, I discuss the ways in which the proposed risk of harm framework advanced by Gratton can overcome the shortcomings of existing approaches under Canadian DPLs. I concur with Gratton that because the risk of harm framework is a flexible and context-based approach, it would ensure that only data presenting a risk of harm to individuals was protected, while facilitating the free flow of data that does not present such a risk. It would thus more effectively promote the function of “personal information” as the gatekeeper to the protection of Canadian DPLs in light of these statutes’ stated purpose. To demonstrate how the proposed risk of harm framework might achieve this in practice, I have applied it to a sampling of cases in which
Canadian decision-makers apply expansionist interpretive approaches to decide whether new data types, or data collected, used or disclosed through new technologies, qualify as “personal information”. I focus on cases involving new data types and technologies that have been posing significant challenges for data protection regulators and causing considerable concern and discussion in the field, namely, GPS, IP addresses, cookies, and unique device identifiers. In analysing these cases using the risk of harm framework, I have demonstrated how this more flexible, nuanced approach overcomes issues of under- and over-inclusiveness, uncertainty, and obsolescence associated with existing interpretations, and better promotes the objectives of DPLs as a result.

Considering whether the proposed risk of harm framework is a desirable substitute for existing expansionist approaches to identifying “personal information” is particularly timely in light of two notable developments in the EU. First, in a 2014 draft report, the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) called on the European Commission to review whether the PIPEDA meets the “adequacy” standard for international data transfers under the EC Directive on Personal Data Protection. The report states that, “[d]epending on the findings of any EU review of PIPEDA, one option would be to ‘suspend or reverse’ the EU’s current formal endorsement of PIPEDA for the legal ‘adequacy’ of the protections it extends to EU citizens doing business with Canadian companies”.

As reported by the Ottawa Citizen, “[l]oss of the adequacy determination will be a major blow to data-sharing between Canada and the EU and will lead to all companies having to negotiate individual contractual arrangements with their EU counterparts — for example IBM Europe and IBM

---

Canada — to safeguard all personal information up to the EU standard before any data transfer can take place.”532

The second notable development is the very recent decision of the EU Court of Justice (CJEU) in Schrems v Data Protection Commissioner533. Importantly, among other rulings, the CJEU in Schrems held that “the supervisory authority in each EU Member State has the right to review whether non-EU countries provide adequate data-protection policies to permit cross-border data transfers”534 under the EC Directive on Personal Data Protection. Importantly, the CJEU ruled that “while the supervisory authority of each Member State cannot invalidate an EU Commission decision acknowledging the existence of adequate protections, it has the right to examine such findings on adequacy with respect to complaints before it.”535 This finding “deviates from the traditional view that a decision by the EU Commission that a particular non-EU nation has adequate data protection laws is conclusive.”536 Thus, the CJEU's ruling that “supervisory authorities of EU Member States are entitled to examine findings of adequacy will permit supervisory authorities to conduct an independent analysis of PIPEDA’s adequacy going-forward.”537 These assessments are likely to be undertaken in light of the widening chasm between PIPEDA and rapidly developing EU laws.538 Because the proposed risk of harm framework enhances the protection of personal information under Canadian DPLs while

532 Ibid.
533 Schrems v Data Protection Commissioner, [2015] EUCJ C-362/14 (06 October 2015) [Schrems].
535 Ibid.
536 Ibid.
537 Ibid.
538 Ibid.
facilitating the free flow of information for trade and commerce purposes, it ought to be viewed
as a desirable reform by individuals, industry players, and data protection regulators alike in the
face of these anticipated assessments.

The potential benefits of this proposed reform to stakeholders should not be overlooked. The
case studies in this thesis illustrate how the proposed risk of harm interpretation of “personal
information” can serve to enhance the protection individuals enjoy under Canadian DPLs.
Specifically, the proposed framework corrects situations where potentially harmful information
might not presently fall within the scope of these laws at all due to the shortcomings of existing
interpretive approaches that have come to light over three decades of technological advancement.
The case studies also demonstrate how the risk of harm framework can serve to further the
business interests of industry players such as employers, internet service providers, broadcasters,
as well as computer and information technology companies (e.g., Facebook, Apple, Microsoft,
Google, etc.) by curtailing the over-inclusiveness of existing approaches. The proposed approach
does this by removing “benign” information (i.e., information that is not potentially harmful to
the individual in the context at hand) out of the domain of data protection legislation such that
businesses and employers can collect, use, and disclose such information without undue
impediment. Using the risk of harm approach recommended here could also be attractive to
regulators whose mandate it is to carry out the objectives of our DPLs since this new framework
is better suited to striking the balance these laws seek to achieve between business interests and
the right to privacy protection.
Since only three decades have passed since the Canadian government first took formal steps to recognize the need for data protection by signing the OECD Guidelines, the country’s data protection regimes are still in their early stages. Accordingly, possible future research directions abound. I have confined my discussion in this thesis to the interpretation of “personal information” under Canada’s private sector DPLs. However, examining how our private and public sector DPLs interact is becoming ever more essential in light of increased outsourcing of public services, public-private partnerships, and other related developments. As Loukidelis writes, how our private and public DPLs “work together to ensure the safeguarding of our personal information, while enabling new forms of service delivery, will continue to be a challenge for policy-makers and legislators.” As a result, a worthwhile future research direction in the field would be to critically appraise the existing approaches to interpreting “personal information” under Canada’s public sector access to information and protection of privacy statutes.

Two divergent approaches under Canada’s public sector DPLs are the relative expansionist interpretation used under the BC FIPPA and the “zone of privacy” approach used under Canada’s federal public sector DPL. I have contended throughout this thesis that BC’s relative approach falls short in light of the BC PIPA’s purpose and developing technologies, and have briefly asserted that the “zone of privacy” approach is vulnerable to the same types of inadequacies as those outlined here in relation to our private sector DPLs. However, a careful and comprehensive analysis would be a worthy pursuit, including discussions on whether it is

539 Power, supra note 2 at v.
540 Ibid.
541 BC FIPPA, supra note 327.
desirable or appropriate to interpret “personal information” in the same manner under both public and private DPLs, and whether the risk of harm framework would be a suitable substitute in both sectors.

These types of analyses would be particularly relevant in light of Canada’s Bill C-51, Anti-Terrorism Act, 2015\(^\text{542}\), which received Royal Assent in June 2015 and enhances the Government’s ability to share information between Government departments and agencies for national security purposes. This includes the sharing of personal information collected by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act\(^\text{543}\) (PCMLTFA) from organizations such as financial institutions; insurance companies, brokers and agents; accountants; securities dealers; casinos; real estate brokers, agents and developers; and money services and remittances businesses. Long before the Anti-Terrorism Act, 2015 expanded the government’s personal data handling powers, the OPCC expressed its concerns about the privacy-intrusive measures of the PCMLTFA, stating that it is “an inherently intrusive Act at odds with the protection of privacy” because it “treats everyone as a potential suspect, weakens existing privacy protections, and enlists a wide range of businesses and professionals in the fight against money laundering and terrorist financing by requiring them to monitor the activities of their customers and make judgments about their behaviour.”\(^\text{544}\) The BC Civil Liberties Association has expressed similar

\(^{542}\) Bill C-51, the Anti-terrorism Act, 2015, 2nd Sess, 41st Parl, 2015 (assented to 18 June 2015).

\(^{543}\) Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17.

\(^{544}\) Regarding financial monitoring regime in Canada: Submission of the Office of the Privacy Commissioner of Canada in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Non-Parliamentary Submissions by the OPC on Privacy Issues (Office of the Privacy Commissioner of Canada, 2007), online: <https://www.priv.gc.ca/information/research-recherche/sub/fmr_071107_e.asp> (accessed 19 October 2015).
concern about the government’s powers under the PCMLTFA to obtain “a great deal of personal information for investigatory purposes without requiring the government to get a warrant or show reasonable grounds to get the information.” In light of the interplay between the Anti-Terrorism Act, 2015, the PCMLTFA and the federal public sector DPL, i.e., the Privacy Act, examining how the proposed risk of harm approach could serve to enhance the protections under the latter would be a particularly worthwhile direction for future research.

Further, looking more broadly at trans-border data flows and cross-border enforcement in the context of international trade, commerce and migration, we can anticipate further efforts and proposals to modernize and harmonize DPLs on a global scale. Given its centrality to these legislative instruments worldwide, the meaning of “personal information” will surely continue to feature prominently in these discussions. Thus additional future research further examining whether the risk of harm framework would be a desirable approach to adopt under DPLs outside of the EU and Canadian contexts would also be a worthy pursuit. Owing to its flexibility, and focus on statutory purpose and risk of harm, this new approach promises to better prevent DPLs from unduly impeding the free flow of information around the globe while enhancing the protections these laws actually seek to afford.

Bibliography

Primary Sources

Legislation

Access to Information Act, RSC 1985, c A-1.

An act to establish a legal framework for information technology, CQLR, C C-11

An act respecting the protection of personal information in the private sector, CQLR C P-391

Civil Code of Québec, SQ 1991, c 64.


Freedom of Information and Protection of Privacy Act, RSBC, c 165.

Interpretation Act, RSBC 1996, c 238.

Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A.

Personal Health Information Act, SNL 2008, C P-701

Personal Health Information Privacy and Access Act, SNB 2009, C P-705

Personal Information Protection Act, SA 2003, c. P-6.5.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSC 1985, c P-21.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17.

Bills

Bill 38, the Personal Information Protection Act, 4th Sess, 37th Parl, British Columbia, 2003 (first reading 30 April 2003).

Bill C-51, the Anti-terrorism Act, 2015, 2nd Sess, 41st Parl, 2015 (assented to 18 June 2015).
Jurisprudence

Europe


Canada

Courts

_Air Canada c Constant_, [2003] JQ 11619 (Que SC).

_Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401_, 2013 SCC 62.

_Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board)_ 2006 FCA 157, leave to appeal denied, [2006] SCCA No 259.


_Citi Cards Canada Inc v Pleasance_, 2011 ONCA 3.

_Dagg v Canada (Minister of Finance)_ , [1997] 2 SCR 403.

_Edmonton (City) v Alberta (Information and Privacy Commissioner)_ , 2015 ABQB 246.

_Englander v Telus Communications Inc._ , 2004 FCA 387.

_Gordon v. Canada (Minister of Health)_ , 2008 FC 258.

_Jones v Tsige_, 2012 ONCA 32.

_Lawson v Accusearch Inc._ , 2007 FC 125.


_Syndicat de Autobus Terremont Ltee c Autobus Terremont Ltee et Paul Imbeau_, 2010 QCCA 1050.

_Union internationale des constructeurs d’ascenseurs, local 89 c Ascenseurs Kone_, 2012 QCCS 913.
United Food and Commercial Workers, Local 401 v Alberta (Attorney General), 2012 ABCA 130.

Privacy Commissioners


Order F2012-14, [2012] AIPCD No. 36.


Ségal v Centre de services sociaux de Québec, [1988] 1 CAI 186.


Arbitrators


Parliamentary Papers


British Columbia, Legislative Assembly, Hansard 36th Parl, 4th Sess, Vol 18, No 11 (03 April 2000) at 14729 (Hon D Lovick).


British Columbia, Legislative Assembly, Hansard 37th Parl, 4th Sess, Vol 14, No 13 (01 May 2003) at 6415 (Hon S Santori).

British Columbia, Legislative Assembly, Hansard 37th Parl, 4th Sess, Vol 16, No 9 (06 October 2003) at 7199 (Hon S Santori).


**International Materials**

*Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector* (EC, 1974).


**Secondary Sources**

**Books**


Drapeau, Michel W. Drapeau & Marc-Aurele Racicot. Protection of Privacy in the Canadian Private and Health Sectors 2012 (Toronto: Thomson Reuters Canada Ltd., 2011).


**Book Chapters**


**Journal and Periodical Articles**


Gratton, Éloïse. “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) 24:1 Albany Law J Sci Technol 105.


Conference Papers


Websites and Blogs

“Complying with the Personal Information Protection and Electronic Documents Act” (17 February 2014), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/fs-fi/02_05_d_16_e.asp>.

Gratton, Éloïse. “Privacy Law in Quebec – Substantially Similar but Different?”, NYMITY Priv Interviews Experts (November 2012) 1, online: <https://www.nymity.com/about/~media/Nymity/Files/Interviews/2013/2012-11-eloisegratton.ashx>.

“Interpretation Bulletin: Personal Information” (October 2013), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/leg_c/interpretations_02_e.asp>.


Patterson, Brent. “Could PIPEDA be a ‘show-stopper’ for CETA?” (10 January 2014), online: Council of Canadians <http://canadians.org/blog/could-pipeda-be-show-stopper-ceta>.


Other


Regarding financial monitoring regime in Canada: Submission of the Office of the Privacy Commissioner of Canada in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Non-Parliamentary Submissions by the OPC on Privacy Issues (Office of the Privacy Commissioner of Canada, 2007), online: <https://www.priv.gc.ca/information/research-recherche/sub/fmr_071107_e.asp>.

Reidenberg, Joel & Paul Schwartz, Data protection law and online services: regulatory responses (Directorate General XV of the Commission of the European Communities, 1998).


Appendices

Appendix A  Definitions of “Personal Information” in Canadian Private Sector DPLs

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Statute</th>
<th>Statutory Definition of “Personal Information”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td><em>Personal Information Protection and Electronic Documents Act</em>, SC 2000, c 5</td>
<td>“personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.</td>
</tr>
</tbody>
</table>
| Alberta      | *Personal Information Protection Act*, SA 2003, c P-6.5 (declared “substantially similar” to PIPEDA) | (j) “personal employee information” means, in respect of an individual who is a potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of

(i) establishing, managing or terminating an employment or volunteer-work relationship, or

(ii) managing a post-employment or post-volunteer-work relationship

between the organization and the individual, but does not include personal information about the individual that is unrelated to that relationship;

…

(k) “personal information” means information about an identifiable individual;
| BC | *Personal Information Protection Act*, SBC 2003, c 63 (declared “substantially similar” to *PIPEDA*) | "employee personal information" means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment;

"personal information" means information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information; |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Québec</td>
<td><em>An Act respecting the Protection of Personal Information in the Private Sector</em>, CQLR c P-39.1 (declared “substantially similar” to <em>PIPEDA</em>)</td>
<td>2. Personal information is any information which relates to a natural person and allows that person to be identified.</td>
</tr>
</tbody>
</table>
## Appendix B Gratton’s Proposed Decision Tree\(^\text{546}\)

<table>
<thead>
<tr>
<th>DATA-HANDLING ACTIVITY</th>
<th>TYPE OF HARM</th>
<th>TEST TO DETERMINE WHETHER DATA ARE “PERSONAL”</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Data are COLLECTED</td>
<td>Harm: <strong>Subjective</strong> (feeling of being under surveillance)</td>
<td>Since DPLs are not the proper tool to address this kind of harm, information collected should be considered personal information only if it may trigger a risk of harm upon being “disclosed” or “used”. <strong>Please refer to the tests under 2 (Data are Disclosed) and 3 (Data are Used).</strong></td>
</tr>
<tr>
<td>2. Data are DISCLOSED</td>
<td>Harm: <strong>Subjective</strong> (psychological: feeling of humiliation, embarrassment)</td>
<td>To determine whether data are personal, the following three criteria should be taken into account: (1) The data are <strong>“identifiable”</strong> to the individual (the more identifiable, the higher the risk of subjective harm). (2) The data are of an <strong>“intimate nature”</strong> (the more intimate, the higher the risk of subjective harm). (3) The data are <strong>“available”</strong> (the less available it was pre-disclosure or the more available it will become post-disclosure, the higher the risk of subjective harm).</td>
</tr>
<tr>
<td>3. Data are USED</td>
<td>Harm: <strong>Objective</strong> (discrimination, financial, physical harm)</td>
<td>If the use of the data triggers objective harm to the individual, the data should qualify as personal information. In such case, the data will have to be (only) two things: (1) <strong>Accurate</strong> (complete, up-to-date, <em>etc.</em>). (2) <strong>Relevant</strong> for the use. If the use of the data will not create such objective harm (negative impact on the individual), then the data should not qualify as personal information.</td>
</tr>
</tbody>
</table>

---

\(^{546}\) Reproduced from Gratton, *supra* note 6, at 224-225.