An Analysis of the Adequacy of the Canadian Privacy Framework Under the *General Data Protection Regulation*

by

Patrick R. Benjamin

A Thesis submitted to the Faculty of Graduate Studies of
The University of Manitoba
in partial fulfilment of the requirements of the degree of

MASTER OF LAWS

Faculty of Law
University of Manitoba
Winnipeg

Abstract

The purpose of this paper is to determine whether the Canadian data protection regime will be found adequate under the European Union's ("EU") General Data Protection Regulation ("GDPR"). The question above will be analyzed by using both the legal doctrinal and comparative method. In order to reach a conclusion as to adequacy the legal test found in s. 42(2) of the GDPR will be used, which emphasizes adequacy in privacy legislation, oversight mechanisms and national security. This analysis will indicate that the Canadian privacy regime is at risk of being found inadequate. However, the analysis will also show that there are strong arguments to be made for why the Canadian data protection regime is still adequate. Throughout the paper there will be recommendations, which will illustrate ways that the Canadian government can improve its data protection mechanism, in order to increase its odds of being found adequate under the GDPR. Finally, there will be a finding of adequacy and explanation as to why the EU Commission will likely find in Canada's favor.

Preface

This dissertation is an original, unpublished and independent work by the author P. R. Benjamin.

Table of Contents

Methodology and Materials

The methods used for this analysis will be both a legal doctrinal and comparative method. These methods will be used to determine whether or not Canadian privacy laws are adequate under the GDPR. Moreover, they will also be used to support conclusions about how Canada can improve its chances of securing an adequacy judgment. A legal doctrinal analysis involves an analysis of all relevant legislation and case law, with the goal of reaching a legal conclusion related to the matter in question. However, the legal doctrinal method does have its weaknesses, as it focuses primarily on legal sources. Therefore, because the transnational flow of personal information has political implications, this paper will also include relevant political discussions. A comparative analysis involves comparing and contrasting a given item in order to flesh out their similarities and differences, with the objective of supporting a given conclusion or hypothesis. This method is necessary because the purpose of an adequacy assessment is to determine if a foreign privacy framework provides adequate levels of protection. Such an analysis requires a lot of comparing and contrasting of both privacy regimes. Thus, a comparative approach is paramount in assessing and in drawing conclusions about GDPR adequacy. In utilizing a comparative approach, we will assess the degree to which Canadian privacy laws are in line with or deviate from the GDPR. However, there will be no "provision by provision" comparison of data protection statutes. Instead, the essential components of both regimes will be compared, as the EU standard is "essential equivalence" and not a perfect mirroring of its regulation.[1] Finally, this analysis will be conducted from the perspective of an unbiased EU Commissioner whose objective is to determine the adequacy of Canada's privacy framework in comparison to the GDPR as a whole.

[1] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 at paras 73, 74.

Legal Test

In this section, there will be a description of the analytical framework that will be used to determine the adequacy of Canadian data protection laws under the EU's GDPR. The framework is located in s. 45(2) of the GDPR.[2] The evaluation criteria used by the European Commission to assess adequacy are located within this section. According to this section, the Commission must consider the following:[3]

> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) Are there supervisory authorities present that are responsible for enforcing compliance with data protection rules, and for assisting and advising the data subject in exercising their rights?
>
> (c) What international commitments has the country entered into? And what other binding obligations arising from conventions, instruments are they bound by?

This analytical framework provides for a holistic approach to the evaluation of a nations data protection regime. For instance, Article 45(2)(a) places an emphasis not only on the data protection legislation, but it also focuses on national security, the rule of law, enforcement and oversight.

Therefore, based on language used the *Schrems* decision and in s. 45(2) of the GDPR, the court will likely evaluate Canada's privacy scheme using a holistic approach. As a result, this paper will also evaluate the Canadian privacy framework holistically by assessing *PIPEDA*, national security and the enforcement of privacy laws.

---

[2] *General Data Protection Regulation*, European Union, 14 April 2016, at para 45(2) (25 May 2018). [*GDPR*]
[3] *Ibid.*

Introduction

Since the 1980s the European Union ("EU") has led the charge in the realm of data protection. In 1980 it was a EU organisation, named the Organisation for Economic Co-operation and Development ("OECD"), that created the first data protection principles.[4] The OECD published a list of seven recommended principles, with the intent that governments worldwide would incorporate them into their future data protection regimes.[5] These guidelines were endorsed by the United States, although they were never implemented into US law. The EU implemented these principles into their Directive 95/46 in 1995.[6]

Directive 95/46 was a developed as a means of standardizing the way EU nations regulated the use of personal data.[7] Prior to its enactment, the approach to data regulation varied across the EU. This impeded the free flow of data across the EU. In passing Directive 95/46, the European Parliament and Council forced its members to bring their national laws into compliance with the directive. For instance, the Directive required that each member state implement the directives into their domestic law by 1998.[8] In standardizing the approach to data protection, the EU Parliament and Council revolutionized not only the way the EU member states approached privacy, but also how many other nations across the world regulate the use of personal data. The Directive's far reaching impact was the result of a provision within the document, which stated that personal data can only

[4] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, online: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>
[5] *Ibid*; The principles are: notice, purpose, consent, security, disclosure, access and accountability.
[6] Data Protection Directive, European Union, 24 October 1995, (13 December 1995).
[7] *Ibid* at preamble (1).
[8] *Ibid*, art 32.

be transferred to third countries if they are found to have adequate levels of protection.[9] As a result, if a non-EU nation wanted to use the personal data of EU citizens, their data protection regime had be in compliance with the Directive. This resulted in countries developing data protection legislation or agreements in order to use EU personal data.[10] For example, the Canadian government passed the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), and the US government implemented the *International Safe Harbor Privacy Principles*.[11] Both of the documents were found adequate by the EU Commission, which is the body responsible for assessing adequacy.

However, the data protection landscape would undergo further change in 2016 as a result of the EU passing the *General Data Protection Regulation* ("*GDPR*").[12] The *GDPR*'s purpose is three-fold. For one, it was implemented as a legally binding regulation and not a directive. As a result, each the regulation became law for each EU state. Previously, each state was only required to use the Directive as a template for each state's data protection laws. Secondly, the *GDPR* is intended to update the privacy protection framework by adding new concepts and principles. For example, the *GDPR* has implemented new concepts such as data portability rights and the right to be forgotten. Thirdly, the *GDPR* creates a new adequacy assessment regime where a third country must now establish not only that its data protection laws are adequate, but also that its entire data protection framework is adequate as well.[13] Therefore, now countries must show that their

[9] *Ibid*, art 25.
[10] Jennifer McClennan & Vadim Schick, "O, Privacy: Canada's Importance in the Development of the International Data Privacy Regime" (2007) 38 Geo J Intl L : 669–693 at 671.
[11] *Safe Harbor Privacy Principles*, United States, (26 July 2000 | EU recognizes "Safe Harbor Privacy Principles" issued by Department of Commerce).
[12] *Supra* note 2.
[13] *Ibid*, art 45.

legislation, national security measures and oversight mechanisms are in compliance with the *GDPR* principles.

As a result, countries such as Canada are now in a position where they might have to amend their pre-existing legislation, create new agreements or establish that their current regime is in compliance if they want to retain their adequacy status. Each third country's adequacy status is reviewed by the EU Commission periodically.[14] Canada's adequacy status is set to be re-evaluated, as it has yet to be evaluated under the *GDPR*. Therefore, this paper seeks to answer the following questions. Given the current state of Canadian privacy laws, would Canada meet the adequacy requirements of the GDPR if the EU were to undertake an adequacy analysis today? Moreover, should our current privacy laws and national security regime be found inadequate, how can Canada improve its chances of obtaining an adequacy judgment in the future?

These questions will be answered over three parts and each part will be considered together in predicting how the EU Commission will assess Canada's adequacy status under the *GDPR*. Part I will assess whether or not *PIPEDA*, as currently constructed, would be found adequate by the Commission. To do so, this part will compare and contrast the core components of the *GDPR* with *PIPEDA*. Additionally, recommendation will be provided as to how the Canadian Parliament can improve *PIPEDA* to further ensure compliance. At the end of each comparison, a prediction as to that section's adequacy will be provided. Once all core components have been analyzed, a conclusion about *PIPEDA* adequacy as a whole will be provided. Part II will assess whether or not the privacy commissioners responsible for overseeing our privacy legislation are provided

[14] *Ibid*, art 45(4).

adequate oversight powers when compared to the *GDPR*. Firstly, there comparative analysis which will determine how the *GDPR* compares to the Canadian one in terms of privacy legislation oversight. Secondly, the analysis will look at the enforcement mechanisms present within the Canadian privacy protection context. Next, there will be a summary of the discussions surrounding the enforcement of Canadian privacy statutes. Afterwards, recommendations will be made as to how the federal Privacy Commissioner's enforcement powers can be improved. Finally, there will be a determination of how the Privacy Commissioner's enforcement mechanisms might impact an adequacy assessment by the EU Commission.

In Part III, there will be an assessment as to how our national-security framework might impact our adequacy evaluation. To do so, there will be a comparative analysis of the legal protections available to EU citizens under Canadian and American laws. This portion of the analysis will focus on topics such as oversight and the availability of personal redresses. The comparison between the US and Canada is important as the EU Commission has found the current US approach to be adequate based on a recent report. Therefore, by comparing the US with Canada, we can try to predict how the EU might evaluate the Canadian national-security framework. This comparison will be the basis upon which this paper evaluates Canada's national-security regime's adequacy under the *GDPR*.

Finally, after each part has been considered individually, there will be a holistic analysis that address each part together. Based on this analysis, a conclusion will be provided which answer the question of whether or not Canada's privacy framework will be found adequate under the *GDPR*.

Part I: Is *PIPEDA* Adequate in 2019?

In this part, there will be an analysis of Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). There will be a determination as to whether or not *PIPEDA* provides adequate levels of protection in comparison to the GDPR. In this section there will be no provision by provision comparison, as adequacy is determined by using an "essential equivalence" standard.[15] Under this standard, a perfect mirroring of GDPR provision is not necessary. Instead, the Commission must be satisfied that subject matter in question is sufficiently similar. Therefore, in order to determine adequacy, this part will focus on the essential components of the GDPR. These components are as follows: (i) consent, (ii) right of access, (iii) data protection by design, (iv) right to be forgotten, (v) data portability, and (vi) data breach reporting. In analysing each of these components, this section will determine if they are adequately addressed in *PIPEDA*. Furthermore, for each component, recommendations on how *PIPEDA* can improve will be illustrated.

1. PIPEDA and Consent

a. Comparison of Consent Provisions Under *PIPEDA* and *GDPR*

Currently, the model that governs the protection and disclosure of personal information is based on the notion that this information is being traded for services.[16] Thus, the exchange of personal information for services is a contract, whereby the information is disclosed upon receipt of informed consent.[17] This form of data protection is often referred to as the consent model. Both

[15] *Maximillian Schrems v Data Protection Commissioner*, *supra* note 1.
[16] Michael Karanicolas of the Centre for Law and Democracy (CLD): (2016 Report).
[17] *Ibid.*

PIPEDA and the *GDPR* utilize the consent model as means of protecting personal information. In this part, the *PIPEDA* rules surrounding consent will be discussed and compared to those present within the GDPR.

(i.) *PIPEDA's* Basic Principles of Consent

The basic principles for consent under *PIPEDA* are found in Principle 3 of Schedule 1 in the Act.[18] This section states that "knowledge and consent" by an individual is "required for the collection, use, or disclosure of personal information, except where inappropriate."[19] According to this section, in order to satisfy the knowledge and consent criteria, organizations must "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used".[20] Moreover, to obtain meaningful consent the "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed".[21] Put differently, an individual must "understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting".[22] Furthermore, according to the Act the "form of consent sought may vary depending upon the circumstances and the type of information.[23] In assessing the form of consent required, organizations must considered the sensitivity of the information in question.[24] For instance, the Act stipulates that express consent is desirable where the information is considered sensitive,[25]

[18] *Personal Information Protection and Electronic Documents Act,* SC 2000, c. 5 [*PIPEDA*], Schedule 1 (Principle 3).
[19] *Ibid.*
[20] *Ibid,* schedule 1 at 4.3.2.
[21] *Ibid.*
[22] *Ibid,* s 6.1.
[23] *Ibid,* schedule 1 at 4.3.4.
[24] *Ibid.*
[25] *Ibid,* schedule 1 at 4.3.6

whereas implied consent is desirable where information is considered not to be sensitive.[26] Additionally, the Act requires that organization take into account the "reasonable expectations of the individual". As a result, deception is explicitly prohibited.[27] Further, the Act also states that consent is not permanent and may be withdrawn. For example, the Act states that "an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice".[28] Finally, the Act also contains certain exceptions whereby an organization may collect, use, or disclose personal information without an individual's knowledge or consent.[29] For example, an individual's personal information might not be protected in the event of a medical emergency.[30] Therefore, *PIPEDA* contains a comprehensive description of what constitutes consent and the situations where exceptions are warranted.

(ii.) GDPR's Basic Principles of Consent

According to the *GDPR*, in order for personal information to be processed by an organization it must be done lawfully.[31] For example, according to Article 6(a) personal information may be processed lawfully if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes".[32] However, consent is not the only way that personal information can be processed lawfully. According to Article 6, personal information can processed lawfully if one or more of the listed criteria is satisfied.[33] For instance, if the data is necessary "for

[26] *Ibid.*
[27] *Ibid*, schedule 1 at 4.3.5
[28] *Ibid*, schedule 1 at 4.3.8.
[29] *Ibid*, s 7(1).
[30] *Ibid*, s. 7(2)(b).
[31] *Supra* note 2, art 6.
[32] *Ibid.*
[33] *Ibid.*

compliance with a legal obligation to which the controller is subject", then it would be deemed lawful under the *GDPR*.[34] Therefore, unlike *PIPEDA* the GDPR does not require consent in order for personal information to be processed. Consent is merely one way that information can "lawfully" be processed. However, if consent is used to collect, use, and disclose a data subjects' personal information lawfully, then certain conditions must be met. These conditions are found in Article 7 of the GDPR and are as follows:[35]

> 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

In comparison, the conditions for consent under the *GDPR* do bare a striking resemblance to those found within *PIPEDA*. For instance, both documents place an emphasis on the data controller ability to demonstrate consent.[36] Furthermore, both documents contain provisions that require data controllers to clearly describe what a data subject is consenting to.[37] Additionally, the withdrawal conditions in both documents contain similar language.[38] Notwithstanding these similarities, the two documents do differ with regard to the role of

[34] *Ibid*.
[35] *Supra* note 2, art 7.
[36] *Ibid*; *PIPEDA*, *supra* note 18, ss 6.1, 7(1).
[37] *PIPEDA*, *supra* note 36, s 6.1, schedule 1 at 4.3.2.; *GDPR*, *supra* note 2, art 7.
[38] *GDPR*, *supra* note 2, art 6.3; *PIPEDA*, *supra* note 18, schedule 1 at 4.3.8.

consent in contracts. For example, the GDPR requires that there be an assessment of the role of consent with regard to the performance of the contract.[39] Such a provision does not exist within *PIPEDA*.

However, the most significant difference between the two documents has to do with consent by minors. Currently, *PIPEDA* contains no provisions that deal with consent by minors, whereas the *GDPR* does contain an article assigned to deal this issue. For example, Article 8 of the *GDPR* states that "the processing of the personal data of a child shall be lawful where the child is at least 16 years old" and that where "the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child".[40] Therefore, the European Commission will likely consider *PIPEDA*'s lack of a provision dealing with consent by minors in assessing adequacy.

In summary, *PIPEDA* contains strong statutory language with regards to consent. In comparison with the *GDPR*, both documents contain several similarities. Nevertheless, they differ in the sense that *PIPEDA* contains no provisions that deal with consent by minors. However, this might not be an issue as the standard is "essential equivalence", and for the most part *PIPEDA* and the *GDPR* are substantially similar. The Canadian government should consider implementing an amendment that deals with consent by minors, as it is in the interest of society to protect minors and it would strengthen the odds of obtaining an adequacy judgment. Below there will be a discussion of ways

[39] *Supra* note 2, art 7.
[40] *Ibid*, art 8.

the federal government can improve consent within *PIPEDA*, with the goal of improving the odds of obtaining an adequacy judgment.

b. Recommendations to Improve the Consent Framework Within *PIPEDA*

In this section, there will be a discussion on ways that the federal government can improve the consent framework within *PIPEDA*. The purpose of this section is to illustrate improvements to the current regime, which could strengthen the likelihood of Canada obtaining a positive adequacy judgment. There will be three different recommendations made. First, this section will advocate for the federal government to amend *PIPEDA* so that it includes a provision that deals with consent by minors. Secondly, there will be a recommendation that a "legitimate business interest exception" be established. Finally, this part will recommend that the "publicly available information" exception be updated to reflect technological change.

(i.) Consent by Minors

The consent-based model while pragmatic for adults can be area of concern for minors. For instance, many youths do not understand the importance of protecting their personal information. Additionally, many experts question whether or not minors possess the ability to adequately consent to the use and disclosure of their personal information. For instance, Owen Charters, the President and Chief Executive Officer of the Girls and Boys Clubs of Canada has stated that children under 13 are simply "too young to understand the implications of data collection and

use".[41] Furthermore, these points were also reiterated by the Office of the Privacy Commissioner ("OPC") in their 2016-17 Annual *PIPEDA* Review Report when the Office stated the following:[42]

> While a child's capacity to consent can vary from individual to individual, we believe that there is nonetheless a threshold age below which young children are not likely to fully understand the consequences of their privacy choices, particularly in this age of complex data-flows. As such, we are taking the position that, in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians. As for youth aged 13 to 18, their consent can only be considered meaningful if organizations have taken into account their level of maturity in developing their consent processes and adapted them accordingly. Our draft online consent guidelines will propose guidance on this issue.

However, despite the OPC's concern over consent by minors, there is no explicit provision within *PIPEDA* that deals with this issue. Therefore, many experts have advocated for the federal government to either create new legislation that protects minors, or amend *PIPEDA* so that there are more stringent rules regulating consent by minors. Some experts have advocated for legislation that prohibits the collection, use and disclosure of personal information stemming from a child under the age of 13. For instance, Owen Charters stated before a Standing Committee that the government should implement a law similar to the US's *Children's Online Privacy Protection Act* ("COPPA"), where parental consent is necessary to collect the personal information of a child under the age of 13.[43] According to Charters, the government should prohibit the collection, use and disclosure of personal information stemming from a child under the age of 13.[44] On the other hand, some experts have advocated for 16 to be the minimum age where a minor can give valid consent. Dennis Hogarth, the Vice President of the Consumers Council of Canada, for instance,

---

[41] House of Commons, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act***,** Report of the Standing Committee on Access to Information, Privacy and Ethics, 42nd Parl, 1st Sess. (February 2018), online: <http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12>.
[42] Office of the Privacy Commissioner, *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*, Children and Youth (21 September 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1-3-3>.
[43] ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1535 (Owen Charters).
[44] *Ibid.*

has stated that "information collected from children under the age of 16 should be prohibited, unless authorized by a legal guardian" and that "protections for children included in the general data protection regulation, GDPR, should be considered for inclusion in any revisions planned for PIPEDA".[45] However, despite these arguments, some believe that creating a minimum age of consent is pointless. Michael Karanicolas, Senior Legal Officer for the Centre for Law and Democracy, for instance is of the view that age of minimum consent provisions are unworkable in practice, and that the focus should instead be on regulating sites that target children.[46]

Thus, the above illustrates that there is a clear interest in protecting the information of minors, although experts disagree on how such protections should be implemented. If the Canadian government is interested in securing an adequacy judgment under the *GDPR*, they should consider implementing a minimum age of consent provision in *PIPEDA* or under new legislation. This would align *PIPEDA* with the *GDPR*, while, at the same time, it would address a legitimate public interest in protecting the privacy of children.

(ii.) Legitimate Business Interest Exception

The legitimate business exception is another way that *PIPEDA* might be improved. A legitimate business exception in *PIPEDA* could be modelled after the exception found in the *GDPR*. Currently, the *GDPR* states that data is lawfully processed where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such

[45] ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1555 (Dennis Hogarth, Vice-President, Consumers Council of Canada).
[46] ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1635 (Michael Karanicolas).

interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".[47] The *GDPR* further states that "a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place".[48] Thus, the *GDPR* provides EU businesses with the ability to process data if they can establish that a legitimate interest exists, which is not overridden by the interest and fundamental right of the data subject. However, under *PIPEDA* no such exception currently existence. For instance, *PIPEDA* provides that an organization shall not "require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes".[49] *PIPEDA* further states that "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances".[50] Thus, under *PIPEDA* the use or disclosure of information must be "explicitly specified" and does not include an exception for legitimate interests.

Some have argued that *PIPEDA* should contain such exception, as express consent can be difficult to obtain under certain circumstance, and can as a result impede business.[51] Linda Routledge, a Director at the Canadian Bankers Association, has suggested that Parliament consider the following:[52]

> We suggest that one way to address this concern may be to streamline privacy notices so that consent is not required for uses that the individual would expect and consider reasonable. In particular, we support the concept that express consent should not be required for legitimate

[47] *Supra* note 2, art 6(1)(f).
[48] *Ibid*, preamble (47).
[49] *Supra* note 18, schedule 1 at 4.3.3.
[50] *Ibid*, art 5(3).
[51] ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Linda Routledge).
[52] *Ibid.*

> business purposes. Some examples of such purposes might include the purposes for which personal information was collected, fulfilling a service, understanding or delivering products or services to customers to meet their needs, and customer service training.
>
> Removing the requirement for express consent for legitimate business purposes would simplify privacy notices, thereby facilitating a more informed consent process where consumers can focus on the information that is most important to them and on which they can take action.

On the other hand, the OPC is of the opinion that a legitimate business exception is not a good idea. For instance, in the OPC's 2016-17 annual report they provided two reasons for why they believe that such an exemption should not exist.[53] For one, the OPC is of the opinion that such an exception is too broad and could be abused by businesses.[54] Secondly, they found that because such an exception is too broad it would capture certain circumstances where an exception is not appropriate.[55]

In conclusion, creating a legitimate business exception might be one way to align *PIPEDA* with the *GDPR*. Currently, *PIPEDA* contains no exception for legitimate interests. Whereas, the *GDPR* repeatedly refers to legitimate interests as a means of lawfully processing personal data. By not including such a provision *PIPEDA* arguably has not kept pace with business innovation and legitimate business concerns. Therefore, to strengthen the privacy framework within Canada *PIPEDA* should be amended to include a legitimate business exception. However, if such a provision were to be implemented into *PIPEDA*, then the concerns listed by the OPC must be addressed. For instance, a legitimate business exception cannot be too broad in order to avoid abuse by the private sector, and so that the exception does not apply to unintended circumstances. Therefore, Parliament should consider implementing such an exception, but the scenarios where

[53] *Supra* at note 42.
[54] *Ibid.*
[55] *Ibid.*

the exception can be used must be clear and unequivocal. If Parliament where do so, then it would increase the odds of *PIPEDA* being found adequate under the *GDPR*.

2. Data Breach Provisions

a. Data Breach Notification Under the *GDPR*

The *GDPR* has implement various improvements to its predecessor, Directive 95/46/EC, such as data breach notifications. Data breach notifications are governed by Article 33 (Notification to the Supervisory Authority) and 34 (Notification to the Data Subject) of the *GDPR*.[56] According to Article 33, in the event of a data breach, "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority" that is "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".[57] Furthermore, in the event that the supervisory authority is not made aware of the breach in 72 hours, the controller must provide a legitimate reason for the delay.[58] However, when it comes to notifying the data subject, the rules are less stringent. For instance, data subject must only be notified of a breach where the "data breach is likely to result in a high risk to the rights and freedoms of natural persons".[59] If the breach is likely to result in a high risk, then the data subject must be notified without undue delay.[60] As illustrated above, the *GDPR* contains an extensive data breach notification framework. These provisions did not exist in Directive 95/46/EC, and are a significant development in the European privacy-protection regime. Therefore, the EU Commission will likely require that a third country have a

[56] *Supra* note 2, arts 33, 34.
[57] *Ibid*, art 33.
[58] *Ibid.*
[59] *Supra* note 2, art. 34.
[60] *Ibid.*

data breach notification framework, which is "essential equivalent" to their data breach notification articles, in order to secure a positive adequacy judgment.

b. Data Breach Notification Under *PIPEDA*

Initially, *PIPEDA* did not contain any data breach notification and reporting provisions. However, in 2015 *PIPEDA* was amended by the *Digital Privacy Act*.[61] The *Digital Privacy Act* implemented a data breach reporting and notification framework. According to this framework, an organization "shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual". [62] Moreover, an individual must only be notified of a breach where "it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual".[63] Finally, according to *PIPEDA* a data breach notification must "be given as soon as feasible after the organization determines that the breach has occurred".[64]

In comparing this framework to the *GDPR*'s, it is apparent that both documents utilize similar language. For instance, both documents require an organization to report a breach to a supervisory authority when a data breach occurs. Additionally, they both require that the individual be notified only where there is a high risk to the individual. However, they do differ in their timing requirements. For example, the *GDPR* has a 72-hour time requirement, whereas *PIPEDA* requires an organization to report "as soon as feasible". Aside from the time of reporting requirements these

[61] *Digital Privacy Act*, SC 2015, c 32; *Supra* note 18 at para 10.1(1).
[62] *PIPEDA*, *supra* note 18, s 10.1(1).
[63] *Ibid*, s 10.1(3).
[64] *Ibid*, s 10.1(6).

provisions are the same. Therefore, the EU commission should not have difficulty finding "essential equivalence" here.

c. Recommendations to Improve Data Breach Framework under *PIPEDA*

Both *PIPEDA* and the *GDPR* contain data breach notification and reporting provisions that are essentially similar. Therefore, the only recommendation would be for *PIPEDA* to implement a data breach notification with a time limit that is less ambiguous. For instance, the "as soon as feasible" language is open for interpretation. Thus, a time limit for notification would improve the efficiency of the data-breach reporting framework. However, implementing such a provision is likely not necessary to obtain an adequacy finding.

3. Right of Access

a. Right of Access under the GDPR

The right to access personal information is an essential component of any privacy-protection framework. In the *GDPR*, the right to access personal information is located in Article 15. According to this article, a data subject has the right to access personal data and to the following information: i) the purpose of processing; ii) the recipient of the personal data; iii) where possible, the amount of time the data will be stored, iv) the right to request that data be erased; v) where information is not collected from the data subject, information as to where it data came from.[65]

[65] *Supra* note 2, art 15.

Thus, the *GDPR* contains an article that not only provides access to personal data in the possession of an organization, but also enables the data subject to properly inform themselves as to how the data is being handled.

b. Right of Access under *PIPEDA*

In Canada, the right to access personal information is an essential component to the privacy-protection framework. The right to access personal information is found in both *PIPEDA* (Private Sector) and the *Access to Information Act* (Public Sector). According *PIPEDA*, an individual shall be given access to their personal information, and shall be able to challenge the accuracy and the completeness of the information.[66] Furthermore, the *PIPEDA* necessitates that once a request is made "an organization shall inform an individual whether or not the organization holds personal information about the individual" and they are also "encouraged to indicate the source of this information ".[67] If an organization is in possession of personal information, they must provide access to that information, unless the information falls under one of the exception located within the Act.[68] Moreover, the act requires that the organization in question provide "an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed". [69] *PIPEDA* also requires that an organization be open about how they handle an individual's data. For example, an organization must indicate what personal information is being made available to related organizations.[70] Therefore, *PIPEDA* does provide Canadians

[66] *Supra* note 18, schedule 1 at 4.9.
[67] *Ibid*, schedule 1 at 4.9.1.
[68] *Ibid.*
[69] *Ibid.*
[70] *Ibid*, schedule 1 at 4.8.2.

with the ability to access their personal information. These provisions do provide Canadians with a significant degree of access as to how their personal information is being handled.

As illustrated above, *PIPEDA*'s right to access personal information is quite comprehensive. However, there are significant differences between *PIPEDA* and the *GDPR*'s right to access provisions. For example, the *GDPR* provides the data subject with more access to how their information is being handled. Under the *GDPR*, for instance, a data subject can request that their data be erased, the source of the data, and the length of time that the information will be stored, whereas *PIPEDA* does not provide its data subject with the same degree of access to their personal information. For example, under *PIPEDA* an organization is not required to identify the source of the information; they are only recommended to do so. Additionally, in *PIPEDA*'s right to access section there is no right to request erasure of personal information However, the Privacy Commissioner of Canada has argued that such a right does exist elsewhere within *PIPEDA*, but this view has been criticized by many privacy experts, which will be illustrated later in this section.

In summary, the *GDPR* and *PIPEDA* both contain a right to access personal information. However, *PIPEDA's* right is less comprehensive that the one found in the *GDPR*. For example, *PIPEDA* does not require an organization to provide a data subject with the source of their personal information, but they are recommended to do so. Thus, the *GDPR* takes a broader approach to the right to the access and handling of personal information. Nevertheless, because the standard is "essential equivalence" the EU Commission will likely find that *PIPEDA*'s right to access is essentially equivalent to the *GDPR*. Despite the differences illustrated above, the EU Commission would likely find that *PIPEDA* provides its citizens with an adequate means of obtain information

on how their data is being handled. As a result, the right to access portion of *PIPEDA* is unlikely to be a contentious issue.

4. Privacy by Design

Privacy by Design is a concept whereby privacy considerations are considered at all stages of business development.[71] For instance, a business implementing privacy by design would consider an individual's privacy rights from start to finish while developing and operating a new system. Privacy by design is a concept that was developed by Ann Cavoukian in the 1990s, who was the Information and Privacy Commissioner of Ontario at that time.[72] According to Cavoukian, privacy by design is based on the following seven principles:[73]

(1) Proactive not Reactive; Preventative not Remedial: Privacy by design is characterized by proactive responses that "anticipates and prevents privacy invasive events before they happen".

(2) Privacy as the Default: An individual should not have to take any action to protect their privacy, as privacy protection is built into any IT system or business practice by default.

(3) Privacy Embedded into Design: Privacy must be embedded into the system or business practice, cannot be an after the fact add-on. Additionally, privacy must be essential to the system, but it must not decrease its functionality.

(4) Full Functionality – Positive-Sum, not Zero-Sum: Privacy by design "seeks to accommodate all legitimate interests and objectives in a positive-sum "win- win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both".

---

[71] David Krebs, "Implementing Privacy By Design" (5 November 2018), online (blog): *David Krebs* <https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/implementing-privacy-by-design/>.
[72] Ana Cavoukian, "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", online (blog): *Ana Cavoukian* <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf>.
[73] *Ibid.*

(5) End-to-End Security – Lifecycle Protection: The privacy by design model applies to the entire lifecycle of the data (i.e. from start to finish).

(6) Visibility and Transparency: Privacy by design must ensure that the technology or business practice in question is "operating according to the stated promises and objectives". Moreover, the "component parts and operations" must be visible and transparent to users and providers.

(7) **Respect for User Privacy:** User privacy must be respected by offering measures such as "strong privacy defaults, appropriate notice, and empowering user-friendly options".

Therefore, as illustrated above, these principles provide business with a comprehensive way to approach privacy protection while developing or implementing new products or services.

a. Criticism of Privacy by Design

Privacy by design is a complicated concept which has attracted extensive debate by legal and engineering experts. These criticisms primarily focus on the difficulties of implementing privacy by design in practice. There are three major concerns presented by experts. For one, some argue that the privacy by design principles are too vague, and thus are unworkable in practice. For instance, Gurses *et al.* have stated that "vague definitions of privacy by design seem to be symptomatic of a disconnect between policy makers and engineers when it comes to what it means to technically comply with data protection".[74] For example, they use the vague definition of data minimization in policy documents to illustrate their point.[75] Secondly, some have argued that the gap between policy and the understanding of privacy by design by engineers must be closed.[76] Lastly, it has also been argued that privacy by design is unworkable if it operates using a voluntary

[74] Seda Gurses *et al.*, "Engineering privacy by design" Paper delivered at the Conference on Computers, Privacy & Data Protection, CPDP 2011 (2011) [unpublished], online: <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf>.
[75] *Ibid.*
[76] *Ibid.*

compliance scheme. Rubenstein and Good, for instance argue that "regulators must do more than merely recommend the adoption and implementation of privacy by design".[77] As illustrated above, there are many criticisms of privacy by design, and thus any legislation that implements the concept must address these issues.

b. GDPR: Privacy by Design

Prior to the *GDPR*, complying with privacy by design was not something EU states were obligated to do. However, the *GDPR* has taken a progressive stance and has implemented the concept into Article 25 of the regulation. According to Article 25, the privacy by design requirement includes the following:[78]

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed…

Giovanni Butarelli, the European Data Protection Supervisor, addressed the issue of privacy by design in the GDPR, when before Parliament he stated the following:[79]

> Privacy by design and privacy by default are no longer recommendations. They are now legal grounds and clear obligations for every controller. It means that systems are to be designed with a

[77] Ira Rubenstein & Nathaniel Good, "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents" (2013) 28:1333 BTLJ at 1408, online: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj>.
[78] *Supra* note 2, art 25.
[79] ETHI, Evidence, 1st Session, 42nd Parliament, 13 June 2017, 1240 (Giovanni Buttarelli, Supervisor, European Data Control Supervisor).

> user-friendly and less invasive approach. There are obligations addressed to controllers, but there is a system to make designers, producers, and developers engaged in practice.

Therefore, as illustrated above, privacy by design plays an essential role in the privacy-protection framework of the *GDPR*. Additionally, in comparing the *GDPR* framework with Cavoukian's principles there appears to be a sufficient amount of overlap. For instance, Article 25 requires that appropriate data-protection safeguards be implemented throughout the entire lifecycle of the information. Moreover, Article 25 requires that data processors be preventative and proactive in protecting data. Furthermore, there is a clear emphasis on implementing "appropriate technical and organisational measures", which by default ensures that "only personal data which are necessary for each specific purpose of the processing are processed". This satisfies both the privacy as default and transparency principles. Thus, not only does the *GDPR* contain a privacy by design obligation, it also implements many of Cavoukian's principles into its privacy by design framework.

Finally, the *GDPR* has addressed many of the privacy by design concerns illustrated above. For one, EU agencies and non-GDPR organizations, have tried to bridge the gap between privacy by design policies and the understanding of the concept by engineers of these systems. For example, the European Union Agency for Network and Information Security (ENISA), has released a report called *Privacy and Data Protection by Design – From Policy to Engineering on Implementation*, which explains how privacy by design should be approach both from an engineering and policy perspective.[80] Additionally, certain organization have been created to assist with the implementation of privacy by design. For instance, the IMDEA Institute provides tutorials on how

[80] European Union Agency for Network and Information Security, "Privacy and Data Protection by Design – from policy to engineering" (2014), online (pdf): *ENISA* < https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

engineers should approach privacy by design.[81] Secondly, the *GDPR* has addressed the voluntary compliance concerns, as the *GDPR* makes privacy by design an obligation.[82] Lastly, as illustrated above, the *GDPR* tries to use straightforward language and as a result addresses the vagueness concern.

In summary, the *GDPR* has implemented a privacy by design provision which its members are obligated to comply with. The language used in this article closely resemble Cavoukian's privacy by design principles. Furthermore, the *GDPR* has address many of the privacy by design criticisms in reducing vagueness, by making privacy by design an obligation, and by instructing engineers on how to implement policy. Finally, privacy by design appears to be a critical component of the *GDPR*, based on the EU Data Protection Supervisor's comments, and is likely to be relevant to a positive adequacy finding.

c. PIPEDA: Privacy by Design

Currently, *PIPEDA* contains no provision dealing with the concept known as "privacy by design". However, the absence of such a provision has not gone unnoticed. For instance, the Privacy Commissioner of Canada, Daniel Therrien, has been cited as describing "privacy by design" as being a significant difference between *PIPEDA* and the *GDPR*.[83] Furthermore, some believe *PIPEDA* should be amended to contain such as provision. For instance, in 2018, Canada's House of Commons released a report called *Towards Privacy by Design: Review of the Personal*

[81] Carmela Troncoso, "Engineering Privacy By Design" (2017), online: <https://summerschool-croatia.cs.ru.nl/2017/slides/Engineering%20privacy%20by%20design.pdf>.
[82] *Supra* note 2, art 25.
[83] ETHI Evidence, *supra* note 79.

Information Protection and Electronic Documents Act.[84] This report was produced by the Standing Committee on Access to Information, Privacy and Ethics. In this report, there were several recommendations made by the Committee on how *PIPEDA* could be improved. Prior to the making these recommendations, witnesses discussed the Act before the Committee. One of the recommendations was that *PIPEDA* be amended to include a privacy by design framework.[85] After a discussion on the privacy by design framework present within the *GDPR* the committee stated that "privacy by design is an effective way to protect the privacy and reputation of Canadians" and that the "proactive, integrated approach should be at the heart of any PIPEDA review".[86] Thus, the Standing Committee on Access to Information, Privacy and Ethics clearly believes that a privacy by design framework similar to the one in the *GDPR* is necessary. Additionally, some believe that privacy by design will be a contentious issue when *PIPEDA*'s adequacy is assessed. Raj Saini, a Liberal Member of Parliament, for instance, asked Giovanni Buttarelli about Article 25's impact on adequacy during a special meeting.[87] However, the European Data Control Supervisor did not answer that portion of Mr. Saini's question.

In conclusion, *PIPEDA* should consider implementing a privacy by design framework for several reasons. For one, privacy by design is one of the major differences between the *GDPR* and *PIPEDA*, as a result its implementation could improve Canada's prospect of obtaining a positive adequacy finding. Furthermore, such a framework would improve privacy protection in Canada by forcing private entities to create privacy-based systems. Additionally, *PIPEDA* has been called outdated and this could improve the Act's reputation. However, should such a framework be

[84] *Supra* at note 41.
[85] *Ibid* at 51-52.
[86] *Ibid* at 51.
[87] ETHI, Evidence, 1st Session, 42nd Parliament, 13 June 2017, (Raj Saini, Liberal Member of Parliament).

implemented into *PIPEDA* the following should be present. Firstly, the Act must not contain vague language, as engineers and data processors must understand what is expected of them. Secondly, private entities that are subject to *PIPEDA* must be obligated to comply with a privacy by design provision, so that voluntary compliance is a non-issue.

5. Data Portability

a. GDPR: Data Portability

Data portability is a new privacy protection concept found within Article 20 of the GDPR. According to this article, the right to data portability consists of the following:[88]

> 1. The subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
>
> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
> (b) the processing is carried out by automated means
>
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

As illustrated in Article 20, the right to data portability consists of three main elements. Firstly, it creates the right to receive personal data. Data portability enables a data subject to receive a subset of their personal data, from a data controller, and store that data for subsequent personal use.[89] For instance, the data subject can store this subset of data on a private device, such as a cell phone. Therefore, the right to receive and store personal data enables data subject to reuse and better manage their personal information. Secondly, data portability creates a right to transfer personal

[88] *Supra* note 2, art 20.
[89] *Supra* note 41 at 35-36.

information from one data controller to another. As illustrated by Article 20(1), data subject shall have the right to transmit data to "another controller without hindrance".[90] However, Article 20(2) stated that this right shall only exist where it is "technically feasible" to do so.[91] In order to make this right feasible, recital 68 of the *GDPR* encourages data controllers to "develop interoperable formats that enable data portability".[92] Although, the *GDPR* does not obligate data controllers to "adopt or maintain processing systems which are technically compatible".[93] Thus, the right to transfer personal information between data controllers exists, although feasibility of the transfer might be an issue. Thirdly, data portability allows the data subject to take control of their personal information. As illustrated above, data portability enables a data subject to receive their personal information and have it processed in a manner that they see fit. As a result, the data controller responding to a data portability requests are not responsible for the receiving controller's compliance with the *GDPR*.

In summary, the *GDPR*'s right to data portability has improved the data subject's right to access their personal information. Also, it has enabled the data subject to exercise greater control over their personal information, although the fact that there is no obligation on data processors to have compatible processing systems might create a workability issue. Nevertheless, this new right does provide data subjects with another means of controlling their data, and from a data subject's perspective, this can only be viewed as a positive. Below, there will be a brief discussion on how data portability is viewed by experts.

[90] *Supra* at note 2, art 20(1).
[91] *Ibid*, art 20(2).
[92] *Ibid*, preamble 68.
[93] *Ibid.*

b. Discussion: Data Portability

The *GDPR's* data portability article has been praised by those who desire greater control over their personal data. For instance, the European Data Protection Supervisor has stated that data portability "could enable businesses and individuals to maximise the benefits of big data in a more balanced and transparent way and may help redress the economic imbalance between controllers on one hand and individuals on the other" and that it can foster "competition and consumer protection".[94] Additionally, the European Supervisor also stated that data portability "could also let individuals benefit from the value created by the use of their personal data" and "could also help minimise unfair or discriminatory practices".[95] Others have praised data portability for "enhancing controllership of individuals on their own data".[96] Paul Quinn, a legal scholar at Vrije Univeriteit Brussel, has praised data portability for its potential research benefits.[97] For example, Quinn has stated that "the possibility of data portability is extremely important in citizen science as it allows individuals (or data subjects) to be able move their data from one source to another (i.e. to new areas of scientific research).[98] Thus, based on the discussion above its evident that data portability has been enhancing competition, creating user controllership of data , and for creating potential economic benefits for the user.

[94] European Data Protection Supervisor (EDPS),"Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability, Opinion 7/2015" (19 November 2015) at 13, online (pdf): *Europe Data Protection Supervisor* <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>.
[95] *Ibid.*
[96] Paul De Hert et al., "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" (2018) Computer L and Sec Review 193-203 at 194.
[97] Paul Quinn, "Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?" (2018) 18:2 Global Jurist 81-97 at 81.
[98] *Ibid.*

However, some have criticized it for not being workable in practice, and for creating a sense of false protection. Robert Madge, a British entrepreneur and technologist, for instance has argued the following. Firstly, Madge claims that that the *GDPR* does not create data portability rights for data that is collected indirectly by a data processor.[99] According to Article 20, the right to data portability only applies to information provided to a data controller.[100] Thus, the right to data portability does not provide data subjects with access and control over all their data, and Madge argues that this creates a false sense of control.[101] Furthermore, Madge also argues that because most data controllers use the "legitimate business exception" to obtain data, that this prevents data subjects from exercising their right to data portability.[102] According to Article 20(1), the right to data portability only applies where consent, contract or where processing is carried out by automated means. As a result, if a data controller uses the legitimate business exception, they are not responsible for complying with Article 20. Therefore, the *GDPR* creates a loophole, which can be used to forgo the right to data portability. Additionally, some have argued that data portability does not fall under data protection, but is a competition-law issue, [103] although, this argument is only relevant if the Article is successfully challenged and removed from the regulation, which is unlikely. Moreover, Vanberg has argued that data portability creates security issues, and result in disproportionate costs for small and medium-sized businesses.[104] For instance, Vanberg argues that when data is transferred from one controller to another, access might be granted to the wrong

[99] Robert Madge, "GDPR: data portability is a false promise" (4 July 2017), online (blog): *Medium* <https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629>.
[100] *Supra* note 2, art 20.
[101] *Madge*, *supra* note 99.
[102] *Ibid.*
[103] Inge Graef et al., "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" (2018) 19:6 German L.J. 1359 1359-1398 at 1359-60.
[104] Aysem Vanberg, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?" (2017) 8:1 Eur J Law 1–22.

person, which can compromise the data.[105] Vanberg also stipulates that small to medium-sized businesses are the most susceptible to security breaches during data portability, as they do not have the resources to invest heavily in data security.[106] Graef *et al.* have argued that by "imposing restrictions on the extent to which market players can process personal data, data protection law structures markets and influences the competitive process" and that it raises "entry barriers to the data economy".[107] The criticisms above, illustrate that data portability has several shortcomings such as security, workability and industry concerns.

c. PIPEDA: Data Portability

As illustrated in the right to access section above, both *PIPEDA* and the *GDPR* contain right to access provisions. However, where they differ is the *GDPR* further supplements this right with a right to data portability, whereas *PIPEDA* does not. As a result, some have viewed *PIPEDA*'s lack of a data portability as a potential hurdle to an adequacy finding by the EU Commission. Daniel Therrien, the Canadian Privacy Commissioner, for instance "urged" Parliament to look at implementing data portability, so that Canada can improve its odds of securing an adequacy finding.[108] Dr. Eloise Gratton, a privacy lawyer with BLG LLP, has expressed concerns before Parliament about how data portability and other new rights within the *GDPR* might impact an adequacy finding.[109] Additionally, in 2018 the Standing Committee on Access to Information, Privacy and Ethics released a report titled *Towards Privacy by Design: Review of the Personal*

[105] *Ibid.*
[106] *Ibid.*
[107] *Supra* note 103, at 1386.
[108] ETHI, Evidence, 1st Session, 42nd Parliament, 16 February 2017, 1545 (Daniel Therrien).
[109] ETHI, Evidence, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Dr. Eloise Gratton).

*Information Protection and Electronic Documents Act***,** where the committee recommended that Parliament adopt data portability to be in line with the *GDPR*.[110] Therefore, the opinions above illustrate that there is a concern that data portability might be essential to secure an adequacy finding. Nonetheless, these concerns might be misplaced as the EU Data Protection Supervisor has stated before the Canadian Parliament that committee members "not focus too much on the novelties in the GDPR, such as design, default, and portability. ... We would encourage that there be a global approach and that you not have a sort of point-to-point replication of every single rule.... [T]he restrictions, exceptions, and derogations for law enforcement are more important than design and default".[111] Notwithstanding this, it is hard to criticize those within the legal sector for being concerned. In conclusion, based on the EU Supervisor's statement data portability may not be essential to securing an adequacy finding. However, data portability would increase the odds of securing an adequacy finding and is a substantial improvement in privacy protection. Thus, Parliament should consider implementing data portability. However, if Canada were to implement such a provision into *PIPEDA*, they would have to draft the provision in manner that does not conflict with existing competitions laws, does not create security risks, and does not create loopholes where private enterprises can circumvent the right.

6. The Right to be Forgotten ("RTBF")

The right to be forgotten is based on the notion that an individual should not be stigmatized for past actions that are no longer relevant in contemporary context. The concept draws its origins

[110] *Supra* note 41.
[111] ETHI, Evidence, 1st Session, 42nd Parliament, 16 February 2017, 1245 &1250.

from France's droit à l'oubli, which was officially recognized in 2010.[112] In May 13 2014 the European Court of Justice ("ECJ") further legitimized the right when they ruled against Google in the *Costeja* decision.[113] In the decision, the ECJ ruled that information posted online, which is excessive or no longer relevant to the purpose for which it was collected, may be removed at the request of the data subject.[114] The court supported its ruling by stating that such a right was supported by Article 6(1)(c) to (e) of Directive 95/46, as well as by Article 7 and 8 of the European Charter.[115] At the time, the right to be forgotten was read into pre-existing provisions. However, this changed when the *General Data Protection Regulation* ("GDPR") came into force on May 25th 2018.[116] The *GDPR* implemented an Article that codified the right to be forgotten into EU law. Article 17 of the *GDPR* codified the principles of the *Costeja* decision into the regulation.[117]

Following the *Costeja* decision, implementation of the right to be forgotten has been directed primarily towards Google. As of May 2014, Google has removed 119165 URLs, with the majority coming from Facebook.[118] In implementing the right to be forgotten, Google uses its own evaluation methods to determine whether or not a link should be removed.[119] Recently, Google has been criticized for not removing links from all its domains.[120] Google has responded to this

---

[112] *Charte sur la publicité ciblée et la protection des internautes [Code of Good Practice on Targeted Advertising and the Protection of Internet Users]* France 2010, online: *UFMD* <https://uniondesmarques.fr/l/library/download/5472/20100929_charte_pub_ciblee_protection_internaute.pdf>.
[113] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Google Spain v Gonzalez)* (2014), ECR C-131-12. [*Google Spain v. Gonzalez*]
[114] *Ibid* at para 89.
[115] *Ibid* at paras 93 & 97.
[116] *Supra* note 2.
[117] *Ibid*, art 17.
[118] Google, "Transparency Report: Requests to delist content under European privacy law" (24 September 2019), online: *Google.ca* < https://transparencyreport.google.com/eu-privacy/overview?hl=en>.
[119] *Ibid.*
[120] Michel Finck, "Google v CNIL: Defining the Territorial Scope of European Data Protection Law" (16 November 2018), online: *University of Oxford: Faculty of Law* < https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law>.

criticism by pointing out that removal from non-European domains would violate the laws of other jurisdictions, such as laws that protect the right to freedom of expression.[121] In response to Google's refusal to apply the RTBF globally the French data protection authority (CNIL) ordered Google to apply the right globally.[122] This decision was appealed and heard by the ECJ.[123] Recently, the ECJ held that the RTBF is not required to be applied globally.[124]

Despite the practical hurdles that a RTBF presents, many non-European countries have started to consider implementing a RTBF of their own. For instance, Canada has arguably begun the process of implementing a RTBF in Canada. The OPC has even gone as far as saying that a RTBF already exist within *PIPEDA*.[125] Additionally, some believe that the right to be forgotten was established by the Federal Court in *A.T. v Globe24h.com*.

As illustrated above, the RTBF is a hot point of discussion in privacy law, and its implementation is still at times controversial. However, a in-depth discussion of the right is beyond the scope of this paper, and as result there will be an emphasis on whether or not the right is necessary to obtain an adequacy finding under the *GDPR*. Thus, in this section, there will be an analysis of the *GDPR*'s RTBF. Additionally, there will be a discussion as to whether or not a Canadian RTBF already exists. Finally, there will be a discussion as to whether or not a Canadian RTBF is necessary for an adequacy finding.

---

[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] *Ibid.*
[125] Office of the Privacy Commissioner, *Draft OPC Position on Online Reputation*, De-indexing and Source Takedowns (26 January 2018), online: *Office of the Privacy Commissioner* < https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/>.

a. GDPR: Right to be Forgotten

As illustrated above, the RTBF was officially codified in the *GDPR* under Article 17.[126] This article has implemented many of the principles articulated by the ECJ in the *Costeja* decision. For instance, Article 17(1)(a) states that a data subject may request that information be removed where "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed", which paraphrases what the ECJ ruled in *Costeja*.[127] Furthermore, the *GDPR* has also made some improvements to the ECJ ruling. For example, under the *GDPR,* a data subject can request that data be removed if they withdraw their consent to processing under Article 6(1) or Article 9(2)(a). Additionally, the *GDPR* allows for removal requests where processing is unlawful. Also, the *GDPR* enables a data subject to request removal where there is an objection to processing under Article 21(1) and 21(2) occurs. Thus, the *GDPR* has not only implemented the *Costeja* principles, but it has also provided for more grounds to seek the removal of personal information.

However, the *GDPR* has also included a comprehensive list of exceptions to its "right to erasure", which are located in Article 17(2).[128] According to this article, the RTBF does shall not apply where processing is necessary for: (a) exercising the right to freedom of expression and information; (b) for compliance with "a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; (c) for public

[126] *Supra* note 2, art 17.
[127] *Ibid*, art. 17(1)(a).
[128] *Ibid*, art. 17(2).

interest or public health reasons; (d) or archiving purposes "in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)"; (e) for the "establishment, exercise or defence of legal claims". Therefore, the *GDPR* does contain an extensive list of exceptions, which helps keep the RTBF in check.

b. Does a RTBF Exist in Canada?

In comparison to the *GDPR*, the Canadian approach to the protection of online reputation is less certain. For instance, it can be argued that Canada contains a RTBF similar to the one found in the *GDPR*. Therefore, the purpose of this section will be to examine alleged sources of a Canadian RTBF, address the criticisms surrounding them, and determine whether or not a RTBF already exists within Canada.

I. Case Law: *A.T. v. Globe24h.com* (Federal Court of Canada)

In 2017, the Federal Court of Canada in the *A.T. v. Globe24h.com* decision ruled that a Romanian-based website violated Canadian privacy laws. The Defendant in this case downloaded Canadian judicial and tribunal decisions from CanLII, a website created by the legal profession to provide the public with access to legal materials. These decisions were then posted on the Romanian-based website, and could only be removed from the site by paying a fee.

As a result of this behavior, the Privacy Commissioner of Canada received several complaints about the website, and in June 2015 the OPC released a report stating that the website violated

Canadian privacy laws.[129] Eventually, the Federal Court of Canada decided to hear the case, and a decision was rendered in 2017. In this case, the Federal Court of Canada addressed three key issues: (1) Does Canada have jurisdiction over the website?; (2) Did the defendant violate Canadian privacy laws?; and (3) Can a Canadian court enforce its judgment against a foreign entity? In this decision, the court found that there was a real and substantial connection to Canada, as the materials posted on the website were Canadian; thus the court had jurisdiction.[130] Additionally, they found that the Romanian-based website violated s. 5(3) of *PIPEDA*, as the information was used for an inappropriate purpose. As a result, Canadian privacy laws were violated.[131] The Court ordered that the information be removed by the website, and that the defendant refrain from copying any further Canadian decisions.[132] Due to the approach taken by the Federal Court, some believe that the court might have established a Canadian right to be forgotten.

Michael Geist, a professor at the University of Ottawa, for instance, stated that the *A.T. v. Globe24h.com* has enabled Canadian courts to use declarations to seek the removal of links from a website, and that they "may have created the equivalent of a Canadian right to be forgotten and opened up an important debate on the jurisdictional reach of privacy law."[133] Barry Bookman, a lawyer with McCarthy Tetrault, has even stated that the decision is in line with the *Google Spain*

[129] Office of the Privacy Commissioner, *Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA: PIPEDA Report of Findings #2015-002*, (06 June 2015), online: *Office of the Privacy Commissioner* < https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-002/>.
[130] *A.T. v. Globe24h.com*, [2017] 4 FCR 310, 2017 FC 114 (CanLII).
[131] *Ibid* at para 75-76.
[132] *Ibid* at para 104.
[133] Michael Geist, "Did a Canadian Court Just Establish a New Right to be Forgotten?" (7 February 2017), online (blog): *Michael Geist* <http://www.michaelgeist.ca/2017/02/did-a-canadian-court-just-establish-a-new-right-to-be-forgotten/>.

decision.[134] However, others have questioned whether or not the *Globe24h.com* decision has established a RTBF in Canada. Allen Mendelsohn, a lawyer and professor at McGill University, for example, has pointed out that in the *Google Spain* decision the search engine was forced to remove offending links, whereas in the Canadian decision the court went after the publisher, and for this reason the *Globe24h.com* decision is inconsistent with the EU RTBF.[135] David Fraser, a privacy lawyer with McIness Cooper, has also argued that this decision should not create a strong precedent, as the defendant was not present, and by extension the evidence and arguments were one-sided.[136] Therefore, there is a clear division in the legal community as to whether or not a Canadian right to be forgotten was created by the *Globe24.com* decision. However, should a right to be forgotten be necessary to obtain an adequacy finding, the *Globe24h.com* decision could be used to convince the EU Commissioner that a variation of the RTBF exists within Canada.

II. 2018 OPC Report Advocating for a Right to Be Forgotten in Canada

As illustrated above, a Canadian RTBF may have been established through case law. Nonetheless, even if the *Globe24h.com* decision has not established a RTBF, some have argued that a RTBF might already exist within the current *PIPEDA* framework anyways. For instance, on January 26th 2018, the OPC released a draft policy position, which stated that a Canadian RTBF already existed within *PIPEDA*.[137]

---

[134] Barry Bookman, "PIPEDA's global extra-territorial jurisdiction: *A.T. v. Globe24h.com*" (3 February 2017), online (blog): *Barry Bookman* <https://www.mccarthy.ca/en/insights/blogs/cyberlex/pipedas-global-extra-territorial-jurisdiction-v-globe24hcom>.

[135] Allen Mendelsohn, "Forget the Right to be Forgotten (For Now)" (28 February 2017), online (blog): *Allen Mendelsohn* <http://allenmendelsohn.com/2017/02/forget-the-right-to-be-forgotten-in-canada-for-now/>.

[136] David Fraser, "Did the Canadian Federal Court take the first step to a "right to be forgotten" with a global take-down order?" (7 February 2017), online (blog): *David Fraser* <https://canliiconnects.org/en/commentaries/44665>.

[137] Office of the Privacy Commissioner, *2017-18 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*, Reputation (27 September 2018), online: *Office of the Privacy Commissioner* < https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/>.

According to the draft policy position, *PIPEDA* contains provisions that allow an individual to ask a search engine to "de-index web pages that contain inaccurate, incomplete or outdated information; removal or amendment of information at the source".[138] Furthermore, the draft policy position states that *PIPEDA* protects online reputation through two mechanisms.[139] Firstly, online reputation can be enhanced through a process known as de-indexing. De-indexing is a process where a search engine removes content from its search engine results, such as a webpage, image, or other resource. The second mechanism is referred to as a source takedown. A source takedown refers to the removal of information from a given source. According to the OPC, search engines are subject to the laws under *PIPEDA*, and as a result they must comply with their obligations under the Act.[140] Additionally, private sector actors must also comply with their obligations under the Act, and as result if an individual withdraws consent, then the private actor must destroy any information that is no longer needed. Below, there will be a brief discussion on how *PIPEDA*, according to the OPC, promotes both de-indexing and source takedowns.

(a.) <u>De-indexing</u>

De-indexing only enhances online reputation if the search engines are subject to *PIPEDA*. According to the s. 4(1)(a), *PIPEDA* applies to "every organization in respect of personal information that … the organization collects, uses or discloses in the course of commercial activities".[141] The OPC is of the opinion that search engines are captured by the language of s.

[138] *Ibid.*
[139] *Ibid.*
[140] *Ibid.*
[141] *Supra* note 18, s 4(1)(a).

4(1)(a). For instance, the OPC believes that because search engines display advertisements alongside search results, that this means they are engaging in "commercial activity".[142] The OPC believes that the ads and the search results are linked because one would not exist without the other.[143] Some have argued that, even if *PIPEDA* applied, its journalistic and literary material exception might protect search engine indexing. However, the OPC believes that search engines do not distinguish between these materials, and thus the exception does not apply.[144] Therefore, if the OPC is correct and *PIPEDA* applies, then an individual should be able to ask a search engine to de-index non-relevant information from their search results.

(b.) Source Takedown

There are two different scenarios that can take place when we are considering a source take down, and they are as follows: (i) an individual has supplied the source with the information themselves, (ii) where the individual has not provided the source with the information. Where an individual provides information to a source, they can subsequently request that non-relevant information be removed and destroyed by withdrawing consent.[145] However, where the information is provided by others, an individual does not have the right to request an unqualified removal of the information.[146] *PIPEDA* does still contain certain remedies. For instance, under schedule 1 at principle 4.9.5 an individual can ask that information be amended if the person can establish that it is incomplete, inaccurate, or out of date.[147] Additionally, s. 5(3) can be used to remove

[142] *Supra* note 137.
[143] *Ibid.*
[144] *Ibid.*
[145] *PIPEDA*, *supra* note 18, schedule 1 at 4.5.3.
[146] *Ibid*, schedule 1 at 4.9.5.
[147] *Ibid.*

information if the individual can establish that the information was collected, used, or disclosed for an inappropriate purpose.[148]

In conclusion, the OPC's "Draft OPC Position on Online Reputation" has made strong arguments as to why a RTBF might already exist with *PIPEDA* as it is currently drafted. However, these arguments rest on the notion that search engines are engaged in "commercial activities" and do not fall under the journalistic/literary exception.

(c.) Criticism of the OPC's Draft Position

The OPC's draft position has drawn some criticism from many legal experts. For instance, some have argued that the Privacy Commissioner's reading of *PIPEDA* cannot be considered a fair one.[149] Teresa Scassa, a law professor at the University of Ottawa, pointed out that the OPC's interpretation of *PIPEDA*'s s. 4(1)(a) is "inconsistent with case law", as indexing does not constitute "commercial activity".[150] Scassa used the Federal Court's *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)* decision to defend this point. According to this decision, "if the primary activity or conduct at hand, in this case the collection of evidence on a plaintiff by an individual defendant in order to mount a defence to a civil tort action, is not a commercial activity contemplated by PIPEDA, then that activity or conduct remains

[148] *Ibid,* s 5(3).
[149] Andrea Gonsalves, "Privacy Commissioner's Draft Report on a "Right to be De-Indexed" is Cause for Concern (26 March 2018), online (blog): *Andrea Gonsalves* <https://cfe.ryerson.ca/blog/2018/03/privacy-commissioners-draft-report-right-be-de-indexed-cause-concern>.; *See also*: *Teresa* Scassa, "OPC Report on Online Reputation Misses the Mark on the Application of PIPEDA to Search Engines" (31 January 2018), online (blog): *Teresa Scassa* <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=270:opc-report-on-online-reputation-misses-the-mark-on-the-application-of-pipeda-to-search-engines&Itemid=80>.
[150] *Ibid.*

exempt from PIPEDA even if third parties are retained by an individual to carry out that activity or conduct on his or her behalf".[151] Scassa argues that this reasoning should apply to search engines as well. Andrea Gonsalves, a lawyer with Stockwoods LLP, argues that search engines only facilitate access to public websites, and that these websites are the ones that use, disclose, and collect personal information.[152] Therefore, based on these arguments it is possible that *PIPEDA* does not apply to search engine indexing.

Recently, the OPC has tried to force Google to de-index certain links from their search engine based on complaints filed with the OPC. However, Google has refused to comply with these requests, claiming that the request to do so is unlawful.[153] Google has even obtained an injunction from the United States District Court in California, which states that the OPC's request to de-index is unlawful.[154] As a result, the Canadian Privacy Commissioner, Daniel Therrien, has commenced a reference to the Federal Court in order to determine if Canada privacy laws include a right to be forgotten.[155] Therefore, based on the arguments listed above, it is possible that the Federal Court will find that indexing does not constitute a "commercial activity" captured by the Act.

In summary, the OPC believes that a Canadian RTBF might already exist within *PIPEDA*. However, this is based on two assumptions about search engines. The first assumption is that it

---

[151] *Ibid*; State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada, 2010 FC 736 (CanLII) at para 106.
[152] *Supra* note 149.
[153] Ken Clark, "Google Fails to Amend Canadian De-indexing Injunction Despite California Court Order" (23 April 2018), online (blog): *Ken Clark* <https://www.lexology.com/library/detail.aspx?g=baf6ee19-f1dc-4c92-b094-53ef700a4eb5>.
[154] *Ibid.*
[155] The Canadian Press, "Privacy czar asks Federal Court to settle 'right to be forgotten' issue" (10 October 2018), online (blog): *BNN Bloomberg* < https://www.bnnbloomberg.ca/privacy-czar-asks-federal-court-to-settle-right-to-be-forgotten-issue-1.1150495>.

assumes that indexing constitutes "commercial activity" by these search engines. The second assumption is that these search engines are engaging in the collection, use or disclosure of personal information. Although, if the former assumption is satisfied, then the latter should not be hard to establish. Finally, should the OPC's interpretation of *PIPEDA* be confirmed by the Federal Court or the Supreme Court of Canada, a Canadian RTBF will be recognized under Canadian law. Thus, if these Courts finds the OPC interpretation of *PIPEDA* to be correct, then the EU Commission should have no difficulty finding that Canada has a RTBF that is "essentially equivalent" to the *GDPR*'s Article 17.

c. Is the Right to be Forgotten Necessary for an Adequacy Finding?

The RTBF is one of the most controversial additions to the EU's *GDPR*. Given the rights controversial nature the EU Commission is unlikely to find a countries data protection regime inadequate on the basis that no RTBF right exists. Furthermore, as illustrated above a provision by provision match is unnecessary.[156] As a result, the Canadian privacy framework could be found adequate without a RTBF. Additionally, the EU Data Protection Supervisor has stated that Canada should "not focus too much on the novelties in the GDPR" and that the EU encourages a "global approach".[157] In conclusion, a Canadian RTBF is not necessary for a adequacy finding, but should a RTBF not exist, Canada must be able to establish strong data protection from a "global perspective" to make up for its absence. Thus, despite the fact that a RTBF could be unnecessary, the Canadian Parliament should take steps to implement a RTBF, as this would strengthen the odds that Canada's data protection regime will be found adequate. As illustrated above, Canada has

[156] ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1245 & 1250.
[157] *Ibid.*

arguably already taken steps in implementing such a right through case law, the OPC draft policy position, and through the upcoming Federal Court reference. As a result, Canada might have already put itself in a better position from an adequacy standpoint, as they can argue that a right to be forgotten already exists in Canada.

Conclusion: Analysis of *PIPEDA*'s Adequacy

As illustrated above, the EU Commission must be satisfied that the third country's data protection framework is "essentially equivalent" to the EU's.[158] Therefore, in analysing *PIPEDA* the Commission will determine if *PIPEDA* is "essentially equivalent". However, to achieve this standard *PIPEDA* does not need to undergo a provision-by-provision mirroring.[159] Instead the EU Commission will look at the Act holistically. A holistic approach will likely entail an examination of the essential components of the *GDPR*, such data privacy by design. As a result, the analysis above has assessed each core section of the *GDPR* and has compared these sections to *PIPEDA*. The purpose of this analysis was to assess how *PIPEDA* has addressed these keys areas within the *GDPR*, with the goal of determining each areas impact on an adequacy ruling.

Based on the analysis in this part, Canada will likely obtain a positive adequacy finding. However, there are certain areas of concern. For one, when *PIPEDA* is compared to the *GDPR*, it is apparent that the Canadian privacy framework has not been updated for some time, which has resulted in

[158] *Schrems*, *supra* note 1.
[159] Article 29 Data Protection Working Party, "17/EN WP 254: Adequacy Referential (updated)" (28 November 2017), online: *ec.europa.eu* < http://webcache.googleusercontent.com/search?q=cache:ymgOKk-scioJ:ec.europa.eu/newsroom/just/document.cfm%3Fdoc_id%3D48827+&cd=1&hl=en&ct=clnk&gl=ca&client=safari>.

significant differences between both documents. For example, *PIPEDA* contains no provision deals with privacy by design or data portability. Secondly, privacy by design is a significant obligation within the *GDPR*, and its absence in *PIPEDA* is likely one of the great causes for concern. For instance, under the *GDPR* privacy by design has been described as an obligation for organizations, which illustrates its level of importance. Therefore, the lack of such a provision might be view as significant negative during an adequacy evaluation. Thirdly, *PIPEDA* has not updated their consent-based model since the Act was first passed. For instance, *PIPEDA* contains no alternative means of processing personal information, and it does not contain a consent-by-minors provision. On the other hand, the *GDPR* contains alternative means to process personal information, and it contains an Article that explicitly deals with consent by minors. Finally, some might argue that the absence of a right to be forgotten could cause issues for a *PIPEDA* evaluation. In support, some might argue that the approach to the right taken by the France's privacy authority is reflective of how the EU views the right, and thus such a right is necessary for an adequacy finding. However, the EU Commission will likely understand that the RTBF is too novel and controversial, and as a result it is unlikely to be a contentious area during an adequacy evaluation. Should it be required, Canada could argue that the right already exists both in statute and case law. Notwithstanding these areas of concern, the standard is "essential equivalence" and when comparing the non-novel areas of *GDPR* to those found within *PIPEDA* there are provisions that meet the "essential equivalence" threshold. For instance, for the most part *PIPEDA* and the *GDPR* contain similar consent provisions, with the difference being that the *GDPR* provides a few exceptions that *PIPEDA* lacks. Another example is that *PIPEDA* has implemented data reporting provisions that essentially mirror those found within the *GDPR*. These are just a few examples of how *PIPEDA* is substantially similar to the non-novel areas of the *GDPR*. Additionally, the EU

Commission has told the Canadian Parliament to not focus on the novel areas of the *GDPR*. As a result, it likely will not matter that *PIPEDA* lacks each of a privacy-by-design or data-portability provision.

In conclusion, when evaluating the *Act* holistically the Commission will likely find that *PIPEDA*'s provisions are "essentially equivalent" the comparable provisions found within the *GDPR*. Moreover, when analyzing *PIPEDA* the EU Commission will likely not give significant weight to the fact that *PIPEDA* does not contain the novel provisions found with the *GDPR* given the Commission told the Canadian Parliament "not to focus" on the novel areas of the regulation. Therefore, for these reasons *PIPEDA* is like to be found adequate by the EU Commission. Despite the fact that *PIPEDA* will likely still be found adequate, Canada should still implement the recommendations illustrated under this Part to increase it odds of being found adequate.

Part II: Enforcement Powers of the Privacy Commissioner

In this Part, there will be an analysis of the enforcement powers of the federal Privacy Commissioner of Canada. The purpose of this analysis is to establish whether or not the federal Privacy Commissioner's enforcement powers would be considered "essentially equivalent" to the enforcement mechanisms of the *GDPR*. The analysis will be broken in to three section. The first section will look at the enforcement mechanisms present within the *GDPR*. Secondly, the analysis will look at the enforcement mechanism present with the Canadian privacy-protection context. In this section, a comparative approach will be used to flesh out the differences between the Canadian and EU approaches. Furthermore, there will be a summary of the discussions surrounding the enforcement of Canadian privacy statutes. Afterwards, recommendations will be made as to how the federal Privacy Commissioner's enforcement powers can be improved. Finally, in the last section, there will be a determination of how the Privacy Commissioner's enforcement mechanisms might impact an adequacy assessment by the EU Commission.

1. Enforcement of the GDPR

(i.) Supervisory Authority Enforcement Powers

Under the GDPR, in order to promote enforcement, supervisory authorities have been granted certain powers, such as investigative powers. The powers granted to these supervisory authorities

are located within Article 58 of the *GDPR*.[160] According to Article 58, supervisory authorities have been granted the following powers:[161]

> (1) **Each supervisory authority will have investigative powers**: For instance, they can order the controller and processor to provide any personal data or information necessary to carry out its tasks. Additionally, the authority can review certifications issued under Article 42(7), engage in audits, and can "obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law".
>
> (2) **Each supervisory authority will have corrective powers:** For example, these corrective powers include the ability to: (i.) issue a warning where a controller or processors operation might infringe the regulation, (ii). issue reprimands where a controller or processors operation has violated the regulation, (iii.) require the controller or processor to adhere to a data subject request based on right present within the regulation. (iv.) order the controller or processor to bring their operation into compliance in a specified manner and within a given period of time. (v.) order the communication of a data breach (vi.) impose a temporary or definitive limitation including a ban on processing, (vii.) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 (viii.) to impose administrative fines according to article 83 (ix.) order the suspension of data flows to a recipient in a third country or to an international organisation.
>
> (3) **Each supervisory authority will have the following authorizations and advisory powers:** For instance, each data protection authority will be able to: (i.) issue opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data. (ii.) to issue an opinion and approve draft codes of conduct (iii.) to adopt standard data protection clauses (iv.) to authorise contractual clauses (v.) authorize administrative arrangements (vi.) to approve binding corporate rules.
>
> (4) **Each supervisory authority will have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation**.
>
> (5) **Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII**.

Based on the list above, the supervisory authorities have been granted the ability use a large number of enforcement mechanisms. However, the *GDPR* does require that the powers be subjected to the "appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter".[162] Therefore, drafters were

[160] *Supra* note 2, art 58.
[161] *Ibid.*
[162] *Ibid*, art 58.

cognisant of the powers being granted to these authorities, and have taken appropriate steps to prevent abuse of these powers.

However, these enforcement mechanisms would likely be ineffective without the backing of strong sanctions. Therefore, the sanctioning power of the supervisory authorities is perhaps their most effective enforcement mechanism. As a result, the section below will discuss the sanctioning powers granted to the supervisory authorities by Article 83 of the *GDPR*.

(ii.) Sanctions

In addition to the enforcement powers illustrated above, a supervisory authority may issue sanctions to enforce a violation of the *GDPR*'s articles. The conditions for securing certain sanctions are fond within Article 83. According to Article 83, the following sanctions can be imposed for violating *GDPR* obligations:[163]

1. A warning, which may be issued in the cases of first and non-intentional noncompliance
2. Periodic data protection audits
3. A fine up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of certain obligations found in Articles 8, 11, 25 to 39, and 42, 43 and 41(4).
4. A fine up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of Articles 5, 6, 7, 9, 12-22, 44-49, 58(1)-(2), and any obligation under Chapter IX

This list illustrates the wide array of sanctions presents within the *GDPR*. For instance, data protection agencies can do everything from written warnings to large fines. As a result, the *GDPR*

[163] *Ibid*, art 83.

has ushered in a new era of data protection enforcement, where regulators are now capable of enforcing compliance of both large and small entities through the use of sanctions. A case in point is when the French data protection agency CNIL fined Google €50 million for violating the *GDPR* consent provision.[164] Therefore, the *GDPR* has created a stronger data protection regime by creating harsh enforcement mechanisms, such as sanctions on annual worldwide turnover.

However, despite the fact that Article 83 contains a large list of conditions for sanctions, the *GDPR* anticipated that for some Member States these sanctions would insufficient. Therefore, legislators created Article 84, which enables Member States to create additional penalties for infringement of *GDPR* provisions, so long as the infringement has not be dealt with by Article 83, and the penalties are "effective, proportionate and dissuasive".[165] Thus, not only does the *GDPR* contains an extensive list of punitive sanctions, it also contains a means of establishing additional penalties, should Member State desire to do so.

2. Enforcement of Canadian Privacy Statutes

In Canada the enforcement of *PIPEDA* is the responsibility of the federal Privacy Commissioner and the Federal Court.[166] This model is known as the ombudsman model, The federal Privacy Commissioner, under this model, is authorized to investigate complaints, audit compliance, mediate disputes, make findings public, and create compliance agreements.[167] the Federal Court is authorized to issue *PIPEDA* compliance orders, publish notices, issue corrections, and award

[164] Laura Kayali, "France hits Google with €50 million fine for GDPR violation" (19 April 2019), online: *Politico* <https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/>.
[165] *Supra* note 2, art 84.
[166] *Supra* note 18, ss 11, 14, 18.
[167] *Ibid*, ss 12-23.1(4).

damages.[168] This model is at odds with the order-making model, which used by the *GDPR*, for instance. Below, there will be a comparison of how the *GDPR*'s order-making model contrasts with *PIPEDA*'s ombudsman model.

a. Ombudsman Model (PIPEDA) vs. the Order-Making Model (GDPR)

In comparing both models, it is apparent that the federal Privacy Commissioner contains fewer enforcement powers. For one, under the *GDPR* the supervisory authorities are able to issue sanctions should certain obligations be violated.[169] In contrast, the Privacy Commissioner does not possess the same sanctioning powers. Instead, this power rest in the hands of the Federal Court.[170] However, many believe that the Federal Court has not utilized this power appropriately and that this power should be held by the Privacy Commissioner.[171] Secondly, the Privacy Commissioner does not have the authority to enforce compliance agreements and must apply to the Federal Court to enforce these agreements.[172] Under the *GDPR*, supervisory authorities are capable of both creating compliance agreements and in enforcing these agreements.[173] In summary, the major difference between the two models is that the Privacy Commissioner of Canada has no order-making powers, whereas the supervisory authorities under the *GDPR* do. However, despite this major difference, both models do contain some similarities. For instance, the Privacy Commissioner's investigative powers under *PIPEDA* are similar to those granted to the supervisory authorities under the *GDPR*. Both systems enable their respective authorities to

[168] *Ibid*, s 16.
[169] *Supra* note 2, art 83.
[170] *Supra* note 18, s 16.
[171] ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1545 (Teresa Scassa).
[172] *Supra* note 18, s 17.1(2).
[173] *Supra* note 2, art 58.

conduct audits, obtain information from relevant parties, and enter a premises for the purpose of investigating non-compliance.[174] Additionally, the Privacy Commissioner does have some of the same advisory powers. For example, the Privacy Commissioner can issue opinions before Parliament and enter into administrative arrangements.

In conclusion, the ombudsman model results in an absence of order-making ability for the Canadian Privacy Commissioner. However, this model does contain some similarities to the order-making model. For example, the investigation and some advisory powers are similar. Nevertheless, some believe that the ombudsman model is inefficient and that Canada should move towards an order-making model. The discussion surrounding such a change will be discussed in the section below.

b. Discussion Surrounding Changes to the Current Enforcement Model

The discussion surrounding the enforcement powers of the federal Privacy Commissioner has revolved around whether or not the ombudsman model should be modified to give the Commissioner additional powers. For example, many have argued that the Privacy Commissioner should have order-making powers, and the ability to impose discretionary fines or sanctions. Robert Dickson, a former Saskatchewan Information and Privacy Commissioner, for instance, has argued that an order-making model in combination with the authority to impose penalties could increase the effectiveness of *PIPEDA*.[175] Dickson points out that while he was the Privacy Commissioner of Saskatchewan, he noticed very little compliance with the *PIPEDA* by small to

[174] *Supra* note 18, s 12.1(1); *Supra* note 2, art 58.
[175] ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Robert Dickson).

medium-sized businesses.[176] He has argued that while the current model might work in forcing large organizations into compliance, it is inefficient at promoting compliance across the board.[177] Dickson believes that if an order-making model is adopted, then this will increase the effectiveness of *PIPEDA*.[178] Teressa Scassa, the Canada Research Chair in Information Law, has argued that the Federal Court has been conservative in issuing damage awards for breaching *PIPEDA* provisions.[179] Therefore, Scassa is also of the opinion that the Privacy Commissioner should be able to administer fines, and issue orders.

Daniel Therrien, the federal Privacy Commissioner, on the other hand, has gone a step further and has illustrated why such powers are important. For instance, he has stated that order-making powers are necessary when dealing with "recalcitrants or recidivists", but this will not be the first course of action in most scenarios.[180] For instance, Therrien has stated that the first course of action would be to work with corporations and businesses in order to bring them into compliance, and that order-making powers would only be used as a last resort.[181]

Others have argued that the Privacy Commissioner should be provided with order-making powers in limited circumstances. Dr. Eloise Gratton, a privacy lawyer with BLG LLP, for instance has argued that "any enforcement powers, penalties, or statutory damages should come into play only once a certain practice is clearly illegal and once the organization has been advised of such and is refusing to adjust its business practices".[182] Chantal Bernier, from the Global Privacy and

[176] *Ibid.*
[177] *Ibid.*
[178] *Ibid.*
[179] *Supra* note 171.
[180] ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0855 (Daniel Therrien).
[181] *Ibid.*
[182] ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Éloïse Gratton).

Cybersecurity Groups, has argued that order-making powers should only exist where these is evidence of an organizations negligence.[183]

On the other hand, some have taken the position that Privacy Commissioner should not receive order-making powers.[184] Micheal Karanicolas, a senior lawyer at the Center for Law and Democracy, has argued that order-making powers would create procedural fairness issues, and that such powers are pointless as most corporations already comply with the Privacy Commissioners recommendations.[185] Suzanne Morin, a Vice-President with the Canadian Bar Association's Privacy Law Section, is of the view that a change to the ombudsman model is unnecessary until evidence of the need for such a power is presented.[186] Ms. Morin further explains this point by stating that Parliament should wait and see how the OPC's new power to issue and enforce compliance agreements is operating in practice before they provide the OPC with additional powers.[187]

In conclusion, most experts are of the opinion that the Privacy Commissioner's order-making powers need to be altered. Furthermore, these experts have emphasized the need for the Privacy Commissioner to be able to issue fines and sanctions in order to enforce compliance. Although, some experts have taken the position that the current system is sufficient. These opinions will be taken into account in the recommendation section below.

[183] ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1555 (Chantal Bernier).
[184] ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1530 and 1605 (Michael Karanicolas).
[185] *Ibid.*
[186] ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1640 (Suzanne Morin).
[187] *Ibid.*

c. Recommendations

(i.) Order-Making Power

The first recommendation is that Parliament should provide the federal Privacy Commissioner with order-making powers. This recommendation is based on the following. First, this would align the Canadian and EU approach to enforcement of data-protection legislation. Second, the ability to make orders would streamline the enforcement process. For instance, waiting for the courts to handle enforce is a time-consuming process, which can be abused by non-compliant parties. Moreover, if the OPC had order making ability the office would be taken more seriously by non-compliant parties, the process would also be streamlined. Finally, the current model is insufficient when it comes to promoting compliance by small and medium-sized businesses.[188] Thus, with order making powers the Privacy Commissioner might be able to reach these entities.

(ii.) Sanctioning Power

The second recommendation is that Parliament should provide the Privacy Commissioner with sanctioning powers. These powers are necessary for the following reasons. For one, the Federal Court has been reluctant in using sanctioning power.[189] Therefore, the Federal Court is not providing sufficient deterrence for *PIPEDA* non-compliance. Secondly, should a non-compliance matter come before the Federal Court it could take months or years to resolve. The OPC can address non-compliances more expeditiously. Finally, if the OPC were to have sanctioning powers this would increase deterrence. For instance, if an individual believes that they are more likely to be sanctioned they will take less risks. Thus, should the OPC have sanctioning powers, this might

[188] ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Robert Dickson).
[189] *Scassa, supra* note 171.

alter the risk/reward analysis businesses undergo when determining how compliant with *PIPEDA* they should be.

(iii.) Selectivity

Finally, the last recommendation is that *PIPEDA* be amended so that the OPC can be more selective in the complaints that they investigate. For instance, in its 2017-18 annual report, the OPC argued that they should have the power to select the complaints they pursue.[190] They argued that the current model "does not permit us to be selective as to which complaints merit investigation" and that these "issues must be investigated along with all other complaints that cannot be resolved to complainants' satisfaction through early resolution".[191] Therefore, if the OPC is allowed to selectively pursue investigations that have merit, their resources could be used more efficiently.

In conclusion, this paper recommends that Parliament amend *PIPEDA* to provide the federal Privacy Commissioner with order-making, sanctioning, and selective investigation powers. Furthermore, we recommend that they implement a model similar to the *GDPR*. The reasons for adopting a *GDPR* model is two-fold. For one, *PIPEDA*'s enforcement mechanism would be comparable to the *GDPR*, which could be useful in an adequacy assessment. Secondly, the EU approach has been successfully in promoting compliance by small, medium- and large-sized corporations. Therefore, the EU model has succeeded in many respects where *PIPEDA* has failed. As a result, in order to improve enforcement of *PIPEDA* a model similar to the *GDPR* is necessary.

[190] *Supra* note 137.
[191] *Ibid.*

3. Adequacy of Canadian Enforcement Mechanisms

In assessing the adequacy of Canada's data-protection enforcement mechanisms, the EU Commission will need to be satisfied that the Canadian approach is "essentially equivalent" to the *GDPR*.[192] In this section, there will be an analysis of how the EU Commission might interpret Canada's data-protection enforcement mechanisms. This analysis will focus on two primary areas. Firstly, there will be a discussion as to how Canada's use of the ombudsman model might impact adequacy. Secondly, this section will assess how the efficiency of the OPC in enforcing non-compliance might affect an adequacy finding. Finally, a determination will be made as to how enforcement of data laws might impact the EU Commission's adequacy finding.

(i.) Use of the Ombudsman Model

Based on the analysis above, the primary difference between both data protection regimes is their use of different enforcement models. For instance, Canada's ombudsman model splits enforcement powers between the OPC and the Federal Court.[193] At the same time, the *GDPR*'s order-making model places all enforcement powers in the hands of Member State supervisory authorities.[194] Notwithstanding these differences, the EU Commission is likely to find the Canadian enforcement mechanisms adequate due to their use of the ombudsman model. The EU Commission will likely recognize that the Canadian model provides for the same enforcement remedies as the *GDPR*. For example, under *PIPEDA* the OPC can investigate data breaches, and the Federal Court can issue

[192] *Schrems*, *supra* note 1.
[193] *PIPEDA*, *supra* note 18.
[194] *Supra* note 2, art 58.

damages or levy fines. Additionally, the Commission is unlikely to take offense with the fact that two different bodies are responsible for enforcement, so long as both bodies are "essentially equivalent" in their efficiency, and spending. Therefore, the issue that the EU Commission will likely focus on are: i) how many resources are being placed into protecting privacy rights; ii) how efficient are the Canadian data protection authorities in enforcing data protection laws?; and iii) how does their efficiency compare to the *GDPR*'s? Thus, below there will be an analysis that will answer these questions.

(ii.) OPC's Enforcement Spending

Finally, the EU Commission will likely want to assess if the OPC is investing a sufficient amount of money in enforcing privacy rights. Based on the following analysis, it is reasonable to conclude that the Commission will find that Canada's use of resources in investigating complaints is adequate. The Commission would only need to compare and contrast Canada's budget with the budgets of other EU supervisory authorities to support this conclusion. For example, in 2016-17 the OPC spent $17,261,095 on the protection of privacy rights.[195] Whereas, in comparison the majority of EU Member States supervisory authorities spent below $10,000,000 on privacy protection.[196] Thus, based on the analysis above it is clear that this will not be a contentious issue.

[195] Office of the Privacy Commissioner, *2018-19 Departmental Plan: Office of the Privacy Commissioner of Canada*, Spending and Human Resources (16 April 2018), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2018-2019/dp_2018-19/#heading-0-4-1>.

[196] John Choudhari, "Cataloging GDPR complaints since May 25" (25 June 2018), online (blog): *John Choudhari* <https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/>.

(iii.) Enforcement Efficiency

As illustrated above, the EU Commission will likely find that the Canadian enforcement model is sufficient if it is "adequate" in its efficiency. The Commission will likely compare the Canadian model to the *GDPR* and assess how they compare in terms of efficiency. In conducting this analysis, the EU Commission will likely reach the following conclusions. The EU Commission will likely find that the Canadian enforcement model is less efficient than the *GDPR*. In support of this conclusion, the OPC has admitted in a 2018-19 report that "without the backdrop of powers to order changes or sanction organizations with penalties for non-compliance, organizations can be slow to respond to our investigative inquiries and equally slow to commit to taking corrective action".[197] This is in contrast with the *GDPR*, where the supervisory authorities have the ability to sanction and order changes.[198] As a result, the supervisory authorities are capable of placing more pressure on organization, which in turn increases efficiency. Notwithstanding these differences, the EU Commission will still likely find Canada's data protection enforcement "adequate" as EU citizens will still get similar levels of protection despite the differences in efficiency. Therefore, the lack of efficiency by the OPC will unlikely result in a negative adequacy finding.

(iv.) Adequacy Determination

In conclusion, the EU Commission will likely find that Canada's data-protection enforcement mechanisms are "essentially equivalent" to the *GDPR*. The Canadian model contains a similar enforcement mechanisms as does its European counterpart. However, the only difference is that

[197] *Supra* note 137.
[198] *Supra* note 2, art 58.

these two mechanisms are split between two government entities. As illustrated above, this might affect efficiency but this is unlikely to be enough to impact an adequacy assessment on its own. Secondly, the Canadian government has poured a sufficient amount of resources into enforcing privacy laws. As a result, the EU Commission will likely be satisfied with the investment in privacy protection. However, despite the unlikelihood of a negative adequacy finding, the Canadian Parliament should consider amending our privacy legislation in order to provide the federal Privacy Commissioner with order-making and sanctioning powers. Even if it were unnecessary for an adequacy finding, it would improve compliance with privacy legislation, and would bring us in line with the EU's approach.

Part III: Impact of Canada's National Security on its Adequacy Assessment

In this Part, there will be a comparative analysis, which will assess how Canada accesses and uses the personal data of EU citizens for national security purposes. The Canadian approach will be compared to the American approach. The reason for the comparison is that the EU Commission, the body responsible for adequacy assessments under the *GDPR*, found US Privacy-Shield approach adequate under the *Schrems* criteria.[199] Therefore, the US approach can be used as a template for what the EU Commission is willing to accept as adequate. Thus, in comparing the Canadian approach with the American approach, we can conclude whether or not Canada is likely to obtain a positive adequacy finding.

These analyses will be divided into two sections. The first section will involve a comparative analysis of the Canadian and American approach to both access and use of EU personal information for national security reasons. In the next section, there will be a comparative analysis of the legal protections available to EU citizens under Canadian and American laws. This portion of the analysis will focus on topics such as oversight, and the availability of personal redresses. Next, a conclusion will be rendered as to whether or not Canada's national security approach will be found adequate under the *GDPR*.

[199] COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield *(notified under document C (2016) 4176).* [*US Adequacy Decision*]

A. Access and Use of EU Personal Data by Public Authorities for National Security Purposes

In this section, the comparative analysis will determine how the Canadian approach to the collection, access, use and storage of EU personal data for security reasons compares to the US approach. As asserted above, the American approach was found to be adequate by the EU Commission, and as a result their approach will act as a useful comparable. At the end of this analysis, there will be a conclusion as to whether or not the Canadian approach will be found adequate based on the comparison.

1. US Approach: Collections, Access, Use and Storage of EU Personal Data for National Security Purposes

The US approach to the collection, access, use and storage of EU personal data for national security reasons is governed primarily by the Presidential Policy Directive 28 ("PPD-28").[200] The PPD-28 document is important for several reasons. First, it creates several limitations for US signal intelligence operations.[201] Signals intelligence is the "interception and analysis of communications and other electronic signals".[202] Secondly, it is binding on US intelligence agencies and remains effective despite administration changes.[203] The PPD-28 is binding in the sense that US intelligence agencies are required to create policies and procedures that match its principles. Third, the PPD-28 creates protections for foreign persons as the document on several occasions uses the

[200] United States, Office of the Director of National Intelligence ("ODNI"), *Presidential Policy Directive 28 ("PPD-28* (Presidential Directive), online: *ODNI* < https://www.dni.gov/index.php/ic-legal-reference-book/presidential-policy-directive-28>.
[201] *Ibid.*
[202] Communications and Security Establishment, "Foreign Signals Intelligence" (01 August 2019), online: *Government of Canada* <https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement>.
[203] Sec. 3.5 (h) of E.O. 12333 with n. 1 of PPD-2; See Memorandum by the Office of Legal Counsel, Department of Justice (DOJ), to President Clinton, 29 January 2000. According to this legal opinion, presidential directives have the 'same substantive legal effect as an Executive Order'.

phrase "regardless of their nationality or wherever they might reside".[204] For example, in the preamble the directive states that "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information".[205] Finally, without the principles found in the PPD-28, the US-EU Privacy Shield would not have been found adequate. However, it should be noted that PPD-28 is not the only document responsible for governing the collection, access, use and storage of foreign intelligence. For instance, the *Foreign Intelligence Surveillance Act* ("*FISA*") also restricts how foreign intelligence can be collected.[206]

Therefore, the analysis below will explain how the PPD-28 principles and other American laws impact the collection, use, access, and storage of foreign signals intelligence. The purpose of this analysis is to illustrate the American approach, and explain why the EU Commission found this approach to be adequate.

(i.) Collection of Foreign Personal Information

The collection of foreign personal information during a US signals intelligence operation is governed by the principles found in section 1 of the PPD-28, which are as follows:[207]

a) The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in accordance with the

[204] United States, Office of the Director of National Intelligence ("ODNI"), *Executive Order 12333* (Executive Order), online: *ODNI* < https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333>.
[205] *Supra* note 198, at preamble.
[206] *Foreign Intelligence Surveillance Act of 1978 ("FISA")*, Pub L No 95–511, 92 Stat. 1783 (codified as amended at 50 U.S.C. ch. 36 § 1801).
[207] *Supra* note 200, s 1.

Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives;

b) Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes

c) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

d) Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.

As illustrated by the principles above, there is a strong emphasis on what constitutes a lawful collection. For instance, the principles stress that signals intelligence "shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose". The Office of the Director of National Intelligence ("ODNI") added to this principle by stating that "Intelligence Community element policies should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, selection terms and identifiers)".[208] According to the National Intelligence Priorities Framework, intelligence priorities are determined by high-level policy makers, which informs what selectors should be used.[209] However, it should be noted that these selectors are evaluated on a regular basis to ensure that they are still in line with intelligence priorities.[210]

[208] Official Journal of the European Union, ODNI Representations (Annex VI) p. 3 (US adequacy report), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN#ntr63-L_2016207EN.01000101-E0063>.
[209] *US Adequacy Decision*, *supra* note 199; ODNI Representations (Annex VI), p. 6 (with reference to Intelligence Community Directive 204). See also Sec. 3 of PPD-28.
[210] Signal Intelligence Reform, 2015 Anniversary Report. See also ODNI Representations (Annex VI), pp. 6, 8-9, 11.

Additionally, the PPD-28 principles also emphasize that signals intelligence "shall be as tailored as feasible" and that the United States will look at "the availability of other information" and prioritize that information. This principle alludes to two things. First, it illustrates that there is a prioritisation of targeted over bulk collection. Secondly, it shows that signals intelligence is only used where no other alternative exists.

As illustrated above, the prioritization of targeted collection is not absolute and circumstances do exist where bulk collection is necessary. In these situations, the PPD-28 sets limits as to how bulk collection can occur. For example, the PPD-28 stipulates that information can only be collected in bulk from non-publicly available signals intelligence where it falls into a specific list of six national security purposes, which include: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats.[211] The ODNI has further illustrated how bulk collection is limited by stipulating that it "applies filters and other technical tools to focus the collection on those facilities that are likely to contain communications of foreign intelligence value", which creates a more targeted approach.[212] Therefore, the PPD-28 does allow for bulk collection in limited circumstances. However, this type of collection is limited to certain national security purposes. Further, filters and technical tools are used to limit the collection as much as possible.

[211] *Supra* note 200, s 2.
[212] *US Adequacy Report*, *supra* note 199, para 73.

Finally, it should be noted that *FISA* contains further authorizations for government agencies to carry out signals intelligence. For example, s. 702 enables the US government to establish certain surveillance programs, such as PRISM and UPSTREAM.[213] However, these programs are also required to carry out targeted searches. This was reiterated by the Privacy and Civil Liberties Oversight Board (PCLOB) when they stated that s. 702 surveillance "consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made"[214]

Based on the information illustrated above, the EU Commission found that their approach signals intelligence collection was adequate under the *Schrems* approach. The EU Commission was satisfied that the PPD-28 collection principles satisfied the principles of necessity and proportionality.[215] In their assessment the Commission found that a targeted collection was "clearly prioritized", and that bulk collection was limited to exceptional circumstances, such as technical or operational reasons.[216] Furthermore, they found that even were there was bulk collection it was limited to "specific" and "legitimate" national security purposes.[217] Additionally, the EU Commission was satisfied by the PPD-28 principles due to their binding nature.[218] Finally, the Commission believes that its decision about the US intelligence collection framework is supported by empirical evidence which shows that information gathered through national security letters ("NSL") and *FISA* "only concern a relatively small number of targets when compared to the overall flow of data on the internet".[219] Therefore, this gives Canada a template for what is expected by our intelligence agencies when it comes to information collection.

---

[213] *Supra* note 206, s 702.
[214] PLCOB, Sec. 702 Report, p. 111.
[215] *US Adequacy Report*, *supra* note 199, para 76.
[216] *Ibid.*
[217] *Ibid.*
[218] *Ibid* at para 77.
[219] *Ibid* at para 82.

(ii.) Access and Use of Foreign Intelligence Information

The PPD-28 principle that deals with access to foreign intelligence information is located at s. 4(a)(ii). According to this principle, access is "shall be limited to authorized personnel" who "need to know the information to perform their mission".[220] Furthermore, access to the information must be consistent with the requirements set in "Executive Orders, IC directives, and associated policies".[221] Additionally, the authorized personnel must be subjected to "appropriate and adequate training" in the principles of the PPD-28.[222] Additionally, authorized personnel may only access and use information in a manner "consistent with applicable laws and Executive Orders and the principles of this directive".[223]

On the basis of the rules set forth in these principles, the EU Commission was satisfied with the US rules that govern access to foreign intelligence information. As a result, if Canada can establish that they have similar rules governing access they will likely also be found adequate with regards to access.

(iii.) Storage and Dissemination of Foreign Intelligence Information

The PPD-28 principle that governs the retention of foreign intelligence information is found in s. 4(a)(i). According to this principle, intelligence community elements "shall establish policies and

[220] *Supra* note 200, s 4(a)(ii).
[221] *Ibid.*
[222] *Ibid.*
[223] *Ibid.*

procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities.[224] The US government has stated that this "reasonableness" requirement is intended to balance "their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities".[225] Additionally, information will only be disseminated if it "the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333".[226] In terms of retention, the PPD-28 states that "information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons" and that "Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States".[227]

Based on the principles laid down in the PPD-28 the EU Commission was satisfied that the US rules on retention and dissemination are "adequately similar" to the *GDPR*. Thus, if Canada can establish that they have similar safeguards, then they should be found "adequately similar" as well.

2. Canadian Approach: Collections, Access, Use and Storage of EU Personal Data for National Security Purposes

In this section, the Canadian national security approach to the collection, access, storage and use of EU personal information will be described. This information will then be compared to the

[224] *Ibid.*
[225] *US Adequacy Report*, *supra* note 199, ODNI Representations (Annex VI).
[226] *Supra* note 200.
[227] *Ibid.*

American approach detailed above. The purpose of this exercise is to determine how these two approaches compare, and to draw conclusion on that basis. As described above, the American approach was found to be adequate by the EU Commission. Thus, if the Canadian approach resembles the American approach, then Canada will likely be found adequate in this area of an adequacy analysis as well. However, if the two approach are different this does not necessarily mean that Canada's approach will not yield a positive adequacy finding.

(i.) Collection of Foreign Personal Information

In Canada the collection of foreign intelligence by the Communication Security Establishment ("CSE") is authorized by the *National Defence Act*.[228] According to s. 273.65(1), the Minister (i.e. Minister of Defence) may "for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization".[229] However, this collection is not without its restrictions. For instance, the *National Defence Act* requires that certain conditions be met before any interception can take place. These conditions are as follows:[230]

> **(a)** the interception will be directed at foreign entities located outside Canada;
> **(b)** the information to be obtained could not reasonably be obtained by other means;
> **(c)** the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
> **(d)** satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

[228] *National Defence Act*, R.S.C., 1985, c. N-5, s 273.65(1).
[229] *Ibid.*
[230] *Ibid*, s 273.65 (2).

The *National Defence Act* also stipulates that information may be intercepted by ministerial authorization to protect the computer systems or the networks of the Government of Canada.[231] These interceptions are subject to the same to the same restriction listed above.[232]

The Canadian Security Intelligence Service ("CSIS") is also responsible for the collection information relating to national security.[233] According to the *Canadian Security Intelligence Service Act* the Service shall "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada".[234] However, for the most part, the Service does not conduct signals intelligence on foreign entities, as this is the mandate of the CSE. Although, the Service does have the authority to assist the CSE based on the language present in s. 16(1) and 17(1) of the *Canadian Security Intelligence Service Act*, should the CSE request assistance.[235] As a result, the national security portion of this paper's analysis will not address CSIS, but instead it will focus on the CSE.

In comparison to the US, the CSE's approach to signal intelligence does have some similarities. For instance, the CSE can only intercept communication "for the sole purpose of obtaining foreign intelligence". If we contrast this with the US's directive that states there must be a "foreign intelligence or counterintelligence purpose", then it becomes obvious that both approaches have a similar objective, although where they differ is that the Canadian government has been vague in

[231] *Ibid,* s 273.65(3).
[232] *Ibid,* s 273.65(4).
[233] *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23**,** s 12(1).
[234] *Ibid.*
[235] *Ibid,* ss 16(1), 17(1).

describing how they conduct surveillance. For example, the CSE has stated that it only intercepts communications based on priorities set by the Government of Canada, which are in a Directive issued by the Minister of Defence.[236] Additionally, CSE has stated that its mandate and operations "are clearly and carefully targeted, by law, to the activities of foreign individuals, states, organizations or terrorist groups that have implications for Canada's international affairs, defence or security".[237] These statement do not clarify the approach with any degree of certainty. Conversely, in the United States, the ODNI has stated that these priorities are based on certain discriminants, such as specific facilities or selection terms.[238] Therefore, it is unclear whether Canada uses a similar targeted approach, as CSE has never publicly released this information.

Additionally, the United States has also made it clear that they use a targeted approach by alluding to that fact in PPD-28. In PPD-28 it states that signals intelligence "shall be as tailored as feasible" and that the United States will look at "the availability of other information " and prioritize that information. In comparison, the Canadian government has not produced a similar regulation or guideline that speaks to their approach. However, the *National Defence Act* does state that the CSE will look to non-signals intelligence source first before engaging in this form of surveillance.[239] Notwithstanding this similarity, it does not clarify how the CSE targets signals intelligence when these other sources are insufficient.

[236] Government of Canada, "Foreign signals intelligence" (01 August 2018), online: *Government of Canada* <https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement>.
[237] *Ibid.*
[238] *US Adequacy Report*, *supra* note 199, *ODNI* Representations (Annex VI) p. 3.
[239] *Supra* note 228, s 273.64(1).

In conclusion, it is unclear as to whether or not the CSE engages in targeted surveillance, as the CSE has not provided the public with any evidence that supports this conclusion, outside of a claim that their mandate and operations are "clearly and carefully targeted". Therefore, if Canada is to be found adequate with regards to its collection of EU personal information for national security purposes, it must clarify how they engage in targeted surveillance. The CSE must be able to empirically support that their approach is indeed targeted. However, if their approach is not always targeted (for example, they use bulk collection) like the US, they must be able to justify such collections, and illustrate that this method is highly restricted and only used as a last resort.

(ii.) Access and Use of Foreign Personal Information

Access to information gathered by personnel of the CSE during a signals intelligence operation is governed by both the *Security of Information Act* ("SIA") and the Canadian SIGINT Security Standards ("CSSS"). According to the *Act*, if you are a current or former member of the CSE then you are permanently bound to secrecy.[240] Under the *SIA* a person bound to secrecy is guilty of an offence if he or she communicates special operational information, which includes information received by a foreign entity.[241] Additionally, the *SIA* also stipulate that any person that wrongfully communicates secret information, such as documents and articles, is guilty of an offence.[242] In comparison to the *SIA*, the CSSS does not stipulate how employees are to be punished. Instead the

[240] *Security of Information Act*, R.S.C., 1985, c. O-5, s 8(1)(a).
[241] *Ibid*, s 8(1).
[242] *Ibid*, s 4(1).

CSSS informs CSE personnel as to how signals intelligence must be handled. CSE personnel must undergo CSSS training to engage in signals intelligence.[243]

In comparison to the US approach, the Canadian approach is essentially the same. For instance, both countries require that only authorized personnel access signals intelligence, and that they receive training before doing so. Furthermore, both countries contain policies and procedures that personnel must follow if they have access to signals intelligence. Therefore, based on how both regimes approach access, it is reasonable to conclude that the Canadian approach is sufficiently similar to the US's approach. On top of the similarities listed above, the Canadian Minister can also place certain conditions on access to intercepted communication when he or she provides a ministerial authorization.[244] In conclusion, the EU Commission would likely have no problem with the Canadian approach to accessing EU data for national security purposes, as the EU found the US approach adequate.

(iii.) Retention and Dissemination of Foreign Intelligence Information

The retention of foreign signals intelligence is governed by the *National Defence Act*. According to s. 273.65(2)(d) of the *NDA,* a ministerial authorization may only be granted if the Minister is satisfied that "satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security".[245] Additionally, the Minister may also implement additional

[243] *Government of Canada*, "*SIGINT* Security (CSE)", online: *Government of Canada* <https://www.cse-cst.gc.ca/en/learning-formation/area-region/sigint-security>.
[244] *National Defence Act*, *supra* note 226, s 273.65(5).
[245] *Ibid*, s 273.65(2)(d).

conditions within a ministerial authorization to restrict "the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications".[246] The statutory language above is unclear as to how long information is retained when it is collected for the purposes described in s. 273.62(2)(d). Leaders of the CSE have reassured the public in the past that they do abide by "firm" time limits when it comes to retaining personal information.[247] Therefore, based on the statutory language above the retention of personal information is restricted to certain circumstances, and the retention of this information is subject to "firm" time limits.

In comparison with the US approach, there are some similarities. For instance, under the American approach, the PPD-28 states that intelligence agencies "shall establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities".[248] Additionally, the PPD-28 has also states that "information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States". In contrasting the US with the Canadian approach, the following is clear. Both approaches use language that indicates that protective measures must be in place so that only information pertinent to national security is retained. For example, the Canadian approach states that "satisfactory measures" must be in place, and the PPD-28 indicates that "policies and procedures reasonably designed to minimize the dissemination and retention of personal information". However, the Canadian approach does differ from the US in the sense that the country's privacy legislation and regulations do not stipulate a maximum length of time that

[246] *Ibid*, s 273.65(5).
[247] Colin Freeze, "CSEC won't say how long it keeps Canadians' private data", *Globe and Mail* (04 August 2014), <www.globeandmail.com>.
[248] *Supra* note 200, s 4(a)(i).

information should be retained where there is no nexus with national security. The PPD-28, on the other hand, indicates that the US limits the retention of this type of information to 5 years. Although, the *National Defence Act* does give the impression that this type of information would not be retained at all, as it states that "private communications will only be used or retained if they are essential to international affairs, defence or security".

In conclusion, both the US and Canadian approach limit retention to circumstances where there is a nexus with national security, international affairs or national defence. Moreover, both countries have procedural safeguards in place to prevent unwarranted retention. For example, Canada uses ministerial authorizations and the Americans have certain agency policies in place to regulate retention. Based on the analysis above, the EU Commission will likely be satisfied that the CSE only retains information where there is a nexus with national security or international affairs, which requires a legitimate purpose. The Commission will likely reach this conclusion, as they found the American approach to be adequate based on similar grounds. Finally, there is one recommendation that the federal government should consider, which is that the federal government or the CSE itself should identify how long it retains foreign intelligence information is being held. They should consider doing so, because the Canadian approach is vague as to time, and clarity on this issue could go a long way with the EU Commission as well as increase public confidence in the CSE.

3. Canadian Adequacy Finding with Regards to Collection, Access and Retention

To conclude, the Canadian approach to the collection, access and retention of EU personal data for national security purposes will likely be found adequate. The EU Commission, in reaching this conclusion, will need to be satisfied of the following. First, they will want to know that Canada is

respecting the principles of necessity and proportionality while collecting information.[249] In order to establish this, Canada will need to establish that the CSE engages in a targeted approach and that bulk collection only occurs in limited and justified circumstances. Canada will likely try to establish that they engage in a targeted approach through the following. Canada will emphasize that the CSE only intercepts communication based on priorities set by a Directive issued by the Minister of Defence.[250] They will likely have to identify what these priorities are and how they are determined, as the ODNI had to answer similar questions during the US adequacy-evaluation process. Second, the CSE will illustrate that they use a targeted approach because they must be able to establish that the information could not be obtained via other means.[251] In order to do so, the CSE must be able to establish that they have a certain target in mind. Third, where bulk collection is necessary the *National Defence Act* indicates that measures must be in place so that "private communications will only be used or retained if they are essential to international affairs, defence or security".[252] Thus, this will be used this to establish that the information that is collected must only be used or retained where there is a specific and legitimate national security purpose. Therefore, the EU Commission will likely be satisfied that Canada has enough evidence to support the conclusion that they engage in a "targeted approach" and that bulk collection only occurs for legitimate national security reasons. Nevertheless, the Canadian government will likely have to divulge the way they engage in a target approach. For instance, the Americans, in their evaluation, went into detail as to how they target signals intelligence. The CSE and the *National Security Act* are more vague in describing the Canadian approach. However, this will only be a hurdle if the CSE has been untruthful in describing their approach to signals intelligence.

[249] *US Adequacy Report*, *supra* note 199, para 76.
[250] *Foreign signals intelligence*, *supra* note 233.
[251] *National Defence Act*, *supra* note 228, s 273.65(2)(b).
[252] *Ibid*, s 273.65(2)(d).

In terms of access by surveillance authorities to EU personal information based on signals intelligence operation, the EU Commission has indicated that it wants to be satisfied that appropriate safeguards are in place to limit access to intercepted information. In the US assessment, the Commission was satisfied that only authorized personnel had access to this information and that they were trained appropriately. Canada will not find it difficult to establish that they are meeting this standard. The Canadian government, like the US, limits access to authorized personnel, and these personnel must receive training prior to accessing intercepted communications. Second, authorized personnel are statutorily bound by an oath of secrecy, and there exists several criminal offences within the *Security of Information Act* that punish unauthorized disclosure or access to certain information, which includes intercepted communications. Therefore, Canada will easily satisfy EU Commission that intercepted EU information will not be accessed by unauthorized personnel.

Finally, the EU Commission will need to be satisfied that information not related to national security is not arbitrarily being retained. The US illustrated that their intercepted communications are not retained for more than 5 years if there is not national security nexus. Therefore, Canada will need to establish that the CSE does not retain information unless there is a national security nexus. The federal government will likely identify that the *National Defence Act* stipulates that "satisfactory measures" must be in place to ensure that information is only retained or used where there is national security, international affair or national defence reason.[253] This provision arguably states that no information will be used or retained, unless there exists a national security nexus.

[253] *Ibid*, s 273.65(2)(d).

Furthermore, the government will also illustrate that the Minister of Defence can add additional conditions to further limit retention and use of the intercepted communications.[254] Based on the documents made available to the public, the EU Commission will likely find that intercepted communication are not being arbitrarily retained. However, the EU Commission will likely call upon the CSE to provide the Commission with assurances that intercepted communications are not being detained indefinitely without justification.

B. Legal Protections Available to EU Citizens

1. American Approach to Oversight and Personal Redress

(i). Oversight Mechanisms

The American intelligence community uses several oversight mechanisms to promote accountability and transparency. For instance, the US has many oversight bodies within the executive branch, judicial review under the *Foreign Intelligence Surveillance Act*, and several Congressional committees. Each of these review mechanisms will be assessed below. Afterwards, a summary of the EU Commission adequacy findings will be provided. Finally, in the next section the Canadian approach will be illustrated and compared with the American approach. After this comparison is complete, a conclusion will be rendered as to whether or not the EU Commission will find Canada's oversight mechanisms "essential equivalent" to the *GDPR*.

[254] *Ibid*, s 273.65(5).

Firstly, this section will assess what oversight mechanisms exist within the US executive branch. The US executive branch has created several oversight mechanisms in order to comply with PPD-28 s. 4(a)(iv), which states that the intelligence community "shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information".[255] For example, the executive branch has established Inspectors-General, the PCLOB, civil liberties or privacy officers, and the President's Intelligence Oversight Board. Each intelligence agency has compliance staff, responsible for ensuring that there is compliance within these oversight bodies.[256]

Inspectors-Generals are responsible for overseeing the activities of intelligence agencies.[257] The Inspectors-General are statutorily independent from the agencies they investigate.[258] The *Inspector General Act* authorizes an Inspector General to investigate complaints, such as abuse-of-authority allegations, which are related to intelligence agency activities.[259] Furthermore, Inspectors-General are authorized to conduct audits and investigate programs suspected of violating the law.[260] There investigative powers include access to audits, documents, reviews, and any other relevant material.[261] If an Inspector-General finds that an agency has violated the law or engaged in inappropriate behaviours, the Office of the Inspector-General can issue a non-binding compliance

[255] *Supra* note 200, s 4(a)(iv).
[256] *US Adequacy Report, supra* note 199.
[257] *Ibid*, ODNI Representations (Annex VI), p. 7. See e.g. NSA, PPD-28 Section 4 Procedures, 12 January 2015, Sec. 8.1; CIA, Signals Intelligence Activities, p. 7 (Responsibilities).
[258] *Ibid.*
[259] *Ibid.*
[260] *Ibid*, ODNI Representations (Annex VI), p. 7. See also Inspector General Act of 1978, as amended, Pub. L. 113-126 of 7 July 2014.
[261] *Ibid.*

recommendations for corrective action.[262] These recommendations are placed in a report and are made available to the public and Congress.[263] Congress can, in response, exercise its oversight function.

Additionally, civil liberty and privacy officers exist within several intelligence agencies.[264] These officers have been provided with certain oversight responsibilities. For instance, these officers are primarily responsible for supervising agency procedures to ensure that they are adequately considering privacy and civil-liberty concerns. Furthermore, they try to ensure that intelligence agencies have adequate procedures in place to address privacy and civil-liberty complaints. Also, these officers must periodically report to Congress and the PCLOB and provide information such as the nature of complaints received and a summary of how these complains where handled.[265] Therefore, these officers are responsible for overseeing procedural matters and complaints regarding civil liberties and privacy.

Furthermore, the executive branch's Privacy and Civil Liberties Board is responsible for overseeing the field of counterterrorism policies.[266] This board consist of five members who are appoint by the President for a six-year term.[267] In overseeing the implementation of counterterrorism policy, the board tries to ensure that privacy and civil liberties are being taken

[262] Inspector General Act of 1978, §§ 4(5), 5. According to s 405(b)(3),(4) of the Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 of 7 October 2010, the IG for the Intelligence Community will keep the DNI as well as Congress informed of the necessity for, and the progress of, corrective actions.
[263] *Ibid.*
[264] 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice (including the FBI), the Department of Homeland Security, the Department of Defense, the NSA, CIA and the ODNI.
[265] *US Adequacy Report*, *supra* note 207.
[266] *Ibid.*
[267] *Ibid.*

into account.[268] In conduction a review of an intelligence agency's actions, the Board can investigate records, documents, reports, and any other relevant material. Moreover, the Board also receives reports from all civil liberty and privacy officers. Based on the information it receives, the Board often provides these officers with recommendation.[269] The Board also frequently provides Congressional committees and the President withreports.[270] Thus, the Board acts as an oversight mechanism for both counterterrorism policy and the civil liberties or privacy officers.

The last oversight mechanism that exist at the executive branch level is the Intelligence Oversight Board. This Board is responsible for overseeing the compliance of the intelligence community with the US Constitution.[271] According to Executive Order 12333, if a non-compliance incident occurs within the Intelligence Community, they must report to the Intelligence Oversight Board.[272]

Secondly, as illustrated above, oversight mechanisms also exist within the US Congress. Congressional oversight is conducted by the House and Senate Intelligence and Judiciary Committees.[273] The Committees are responsible for overseeing the administration of justice within federal law enforcement agencies, which includes intelligence agencies.[274] In exercising this oversight, the Committees are authorized to engage in hearings, investigations, and reviews of intelligence programs or events. The objective of these Committees is to submit to the House and Senate respectively proposals for legislation or to create reports for the House and Senate

[268] *Ibid.*
[269] *Ibid.*
[270] *Ibid.*
[271] *Ibid.*
[272] *Supra* note 204.
[273] *Ibid.*
[274] US Senate Select Committee on Intelligence, "Overview of the Senate Select Committee on Intelligence Responsibilities and Activities" (10 October 2019), online: *US Senate* <https://www.intelligence.senate.gov/about>.

respectively regarding intelligence programs.[275] In order to meet this objective the Committees needs access information.

These Committees receive this information through several US statutes. For example, the primary source of this reporting requirement is found within the *National Security Act*. The *National Security Act* requires that Congressional intelligence committees be "kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter".[276] Also, the same Act requires that illegal intelligence activity be "reported promptly to the Congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity".[277]

These reporting requirements have been increased by subsequent acts, such as *FISA*. For instance, *FISA* requires that the Attorney-General inform these intelligence committees about activities that involve certain sections within the Act. *FISA* also stipulates that reports be generated for certain types of *FISA* court proceedings, such as §702 proceedings. Furthermore, the *USA Freedom Act* has also extended the reporting requirements by requiring the federal government to disclose each the number of *FISA* orders and directives sought, as well as an estimate of the number of American and non-American persons targeted by surveillance.[278] Moreover, the *USA Freedom Act* also requires that there be greater public reporting on the number of National Security Letters sought.[279]

[275] *Ibid.*
[276] See Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)).
[277] See Sec. 501(b) (50 U.S.C. § 413(b)).
[278] USA FREEDOM Act of 2015, Pub. L. No 114-23, § 602(a).
[279] *Ibid*, § 602(a), 603(a).

In summary, there are numerous statutory provisions that provide US intelligence committees with information. These provisions ensure that these committees can properly investigate and report on the activities of intelligence agencies.

Thirdly, the last source of oversight stems from judicial authorization and review by a *FISA* court. The *FISA* court is a tribunal that is tasked with making determinations based on *FISA*.[280] The *FISA* court's decisions are reviewable by the Foreign Intelligence Court of Review ("FICR"), and the US Supreme Court. As illustrated above, judicial authorization is one of the primary tasks performed by the *FISA* court. *FISA* requires that intelligence agencies obtain prior judicial authorization before they can engage in certain activities.[281] The process for obtaining a judicial authorization from a *FISA* court is as follows. First, an intelligence agency (e.g. CIA, FBI, NSA) must prepare a draft application, which is sent to National Security Department of the Department of Justice.[282] Next, the National Security Department evaluates the application, and if the application is finalized, then it is sent off to the Attorney General's office for approval by the Attorney-General, Deputy Attorney-General or the Assistant Attorney-General for National Security.[283] Finally, if the application is approved by the Attorney-General's office, then it must go before the *FISA* court where it receives its final approval.[284]

The two primary foreign intelligence authorizations come from s. 501 and 702 of *FISA*. Section 501 of *FISA* is a provision that allows for the collection of "any tangible things" relevant to a

[280] *Supra* note 202.
[281] *Ibid.*
[282] PCLOB, Sec. 215 Report, p. 177
[283] *Foreign Intelligence Security Act*, *supra* note 204, §§ 1804 (a), 1801 (g).
[284] PCLOB, Sec. 215 Report, p. 179

terrorism investigation or clandestine intelligence activities.[285] Thus, s. 501 enables the intelligence agencies to engage in individual surveillance activities. However, in order for an agency to engage in an activity that falls within s. 501, their application to the *FISA* court must contain reasonable grounds to believe that: i) the information sought does not involve a US person; and ii) that its purpose is to protect against "international terrorism or clandestine intelligence activities".[286] Additionally, the court must be satisfied that the application contains sufficient minimization procedures, so that the intelligence collected will not be improperly retained or disseminated.[287]

Section 702 diverges slightly from s. 501 in the sense that the *FISA* court is authorizing surveillance programs under the provision. For instance, this provision was used to authorize programs such as PRISM and UPSTREAM. Section 702 of *FISA* is perhaps the most important foreign surveillance mechanism used by the United States. Under this section, intelligence authorities are authorized to target persons that are "reasonably believed to be located outside the United States to acquire foreign intelligence information".[288] This type of surveillance is undertaken by the NSA. First, the NSA will determine non-US based target or targets that NSA analysts believe will produce valuable foreign intelligence. Second, once the NSA has received approval for targeting a given person or persons, selectors identifying the communication mechanism that will be use are applied.[289] The *FISA* court's role in this process is not to determine that individuals are appropriately being targeted; rather, it is to ensure that the purpose of the

[285] *Supra* note 206, § 1861(a)(1).
[286] *Ibid*, § 1861 (b).
[287] *Ibid.*
[288] *Ibid*, § 1881a (a).
[289] *Ibid*, §1881a (h).

operation is to obtain foreign intelligence information.[290] Additionally, the *FISA* court is also response for reviewing and authorizing program certifications on an annual basis. Additionally, it is the *FISA* court's responsibility to ensure that appropriate minimization procedures are in place, so that information is not unlawfully being disclosed or retained.[291] Furthermore, the Attorney General and the Director of National Intelligence have an obligation to report to the *FISA* court incidences of non-compliance.[292] Therefore, the *FISA* court is responsible for ensuring that the s. 702 surveillance programs are engaging in lawful surveillance.

In assessing the US oversight mechanisms, the EU Commission found that they were "essentially adequate" with the *GDPR*.[293] However, the oversight mechanism that impressed the EU Commission was the creation of a new oversight mechanism known as the Ombudsperson, whose role is to ensure that complaints are properly investigated and address. This mechanism will be discussed in the personal redress portion below.

(ii.) Personal Redress Mechanisms

In this section, there will be a description of the avenues available under US law for EU citizens should they have concerns as to how their personal data is being handled. The purpose of this section is to illustrate the mechanisms used by the US to promote individual redress by EU data subjects, and then compare and contrast this approach with the Canadian approach. The American

[290] *Ibid.*
[291] *Ibid*, § 1881a (i).
[292] Rule 13(b) of the FISC Rules of Procedure.
[293] *US adequacy Decision*, *supra* note 199.

approach is a useful template to compare and contrast with as the EU Commission has found the US approach "adequate" under the *GDPR*. Therefore, if Canada wishes to obtain a similar finding, it would useful to see if they are in line with the us approach. If the Canadian approach is found to be similar to the American approach, which will be discussed below, then Canada should have no problem attaining a positive adequacy finding. The overview of the personal redress mechanisms will be divided as follows. First, there will be a description of the statutory redress mechanisms available. Second, there will be a discussion as to what the US Ombudsperson is and what their responsibilities are. Lastly, there will be a summary of why the EU Commission found the US personal redress mechanisms adequate under the *GDPR*.

(a.) Statutory Personal Redress Mechanisms

There are four American statutes that provide EU data subject with some form of individual redress. Each of these Acts will be discussed briefly below.

First, there is *FISA*, which is the Act that governs foreign surveillance. The *FISA* contains several provisions that enable non-US persons to challenge unlawful surveillance. For instance, *FISA* allows a non-US person to bring forward a civil action for monetary damages where there is grounds to believe that the US unlawfully and willfully used or disclosed personal information about them.[294] Furthermore, a non-US person may also challenge the legality of surveillance information where the US government wants to use that information in a judicial proceeding or administrative hearing against the individual.[295] Additionally, it possible to sue a US government

[294] 18 U.S.C. § 2712.
[295] *Supra* note 206, § 1806.

official personally.[296] Thus, the *FISA* does provide non-US citizens with several redress mechanisms.

Next, there is the *Administrative Procedure Act*, which is the Act that governs how a federal administration may propose and establish procedures.[297] According to this Act, "any person suffering legal wrong because of any agency action, or adversely affected or aggrieved by such action within the meaning of any relevant statute, shall be entitled to judicial review".[298] If this is the case, a non-US person could ask the court to hold unlawful or set aside agency actions, findings, and conclusions found to be "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law".[299]

Thirdly, the US has *Freedom of Information Act*, which is the Act that provides US and non-US actors with the right to access information in the possession of the U.S. government, subject to certain exceptions.[300] Thus, this is another way that non-US citizens can ensure that the U.S. government only has access to information that they are lawfully able to possess. Additionally, it can be used to verify how the US government is using an individual information. It should be noted that the *Freedom of Information Act* does not provide individual with a judicial remedy. Although, the *Act* does enable a non-US citizen to gain access to information which might be pertinent to bringing forward a cause of action under another statute. Nevertheless, the Act does have certain weaknesses, for instance there is an extensive list of exceptions. These exceptions, which includes

[296] *Ibid*, § 1810.
[297] 5 U.S.C. § 702
[298] *Ibid*, s 10(2)(a).
[299] *Ibid*, § 706(2)(A).
[300] 5 U.S.C. § 552.

a restriction on access to information that is classified based on national security grounds, might seriously limit the effective use of this Act.[301]

Finally, the U.S. federal government has passed several statutes that deal with specific forms of data, which provide non-US citizens with an individual redress mechanism. For instance, both the *Electronic Communications Act* and the *Right to Financial Privacy Act* enable non-U.S. citizens to bring forward a cause of action where their rights under these Act have been violated.[302]

In summary, in the U.S., there are several Act that extend individual redress to non-U.S. citizens. Therefore, should an EU citizen find that their information is being used inappropriately or if they want to know what information U.S. authorities have access to, they have several different avenues they can use to address these issues. However, despite the statutory protections available through statutes, the personal redress mechanism the EU Commission emphasized the most was the EU-US Privacy Shield Ombudsperson, which will be discussed below.

(b.) EU-US Privacy Shield Ombudsperson

As illustrated above, the EU Commission placed a significant amount of emphasis on the EU-US Privacy Shield Ombudsperson during their adequacy assessment. The EU Commission was of the opinion that there exist some circumstances where EU citizens did not have any redress, such as when Executive Order 12333 is used.[303] Additionally, the EU Commission found that even where US statutes provided grounds for redress, the allowable causes of action are limited and the

[301] *Ibid.*
[302] 18 U.S.C. §§ 2701-2712; 12 U.S.C. § 3417.
[303] *US Adequacy Decision*, *supra* note 199 at para 115.

individual must be able to establish that they have standing, which can be difficult.[304] Thus, in order to satisfy the EU Commissions concerns they established a Ombudsperson mechanism.[305]

The Ombudsperson is responsible for ensuring that complaints are properly investigated, and that individual receive independent confirmation that they have or have not been complied with.[306] If U.S. laws have not been complied with, the Ombudsperson is responsible for providing confirmation that the non-compliance has been remedied.[307] In order to meet its obligations, the Ombudsperson is authorized to rely on independent oversight bodies with investigative powers, such as the Inspectors-General or the PCLOB.[308] Where non-compliance is found by any of these oversight bodies, the non-compliance must be remedied, so the Ombudsperson can communicate with the EU subject that the issue has been remedied.[309] EU citizens can submit complaints to the Ombudsperson in the following ways. First, an EU citizen can submit a complaint to their Member State's supervisory authority, who will then pass on the complaint to the Ombudsperson.[310] Alternatively, an EU data subject can file a complaint directly with the Ombudsperson.

The EU Commission, in providing its adequacy finding, stated that for the Ombudsperson to be found as an acceptable redress mechanism, the following needs to be present. First, the Ombudsperson must not be instructed by the intelligence community, as independence is necessary to avoid any form of coercion or bias.[311] According to the Commission, this is necessary because

[304] *Ibid.*
[305] *Ibid* at para 116.
[306] *Ibid* at para 117.
[307] *Ibid.*
[308] *Ibid.*
[309] *Ibid* at para 120.
[310] *Ibid* at para 119.
[311] *Ibid* at para 121.

the Ombudsperson must confirm that a complaint has been properly investigated, confirm compliance or non-compliance, and in the event of non-compliance, confirm that the matter has been remedied. They cannot perform this function reliably if they are not an independent body, as there would be a clear bias. Lastly, in order for the Ombudsperson to properly perform their role, the Commission is of the view that they must receive all necessary information, which the US has reassured they will.[312]

Therefore, based on the reasons listed above, the EU Commission found that the U.S. has sufficient oversight and individual redress mechanism in place. Next, there will an analysis that illustrates the Canadian approach to oversight and individual redress, which will be compared and contrasted with the mechanisms listed above. How the two countries compare and contrast will help determine whether or not the Canadian approach to oversight and individual redress will be found adequate.

2. Canadian Approach to Oversight and Personal Redress

(i.) Oversight Mechanisms

The Canadian surveillance program promotes accountability and transparency through statutory protections, an oversight bodies within the executive branch, and judicial review. Each of these oversight mechanisms will be addressed below. Afterwards, these oversight mechanisms will be compared to the American approach. Finally, based on the comparison a conclusion will be

[312] *Ibid.*

provided as to whether or not Canada's oversight mechanisms are "adequate" under an adequacy review.

(a.) Statutory Oversight Mechanisms

The Canadian foreign surveillance regime is governed by the *National Defence Act* and the *Privacy Act*, which includes several safeguards.[313] First, the safeguards established by the National Defence Act will be assessed. The *National Defence Act* is the piece legislation that establishes how the CSE can go about intercepting foreign communications. Next, the *Privacy Act* safeguards will be discussed in detail. The *Privacy Act* governs how government agencies can collect, retain and use personal information.

As illustrated above, the *National Defence Act* establishes what constitutes an acceptable form of foreign communications surveillance. In doing so, the *Act* establishes several safeguards to ensure that the CSE is subjected to sufficient oversight in conducting foreign surveillance activities. For instance, s. 273.65(1) of the *National Defence Act* requires that the CSE receive ministerial authorization before they can intercept any foreign communication.[314] According to this section, certain safeguards must be in place to receive ministerial authorization. For example, the CSE must be able to establish that:[315]

> **(a)** the interception will be directed at foreign entities located outside Canada;
> **(b)** the information to be obtained could not reasonably be obtained by other means;
> **(c)** the expected foreign intelligence value of the information that would be derived from the interception justifies it; and

[313] *National Defence Act*, *supra* note 228; *Privacy Act*, *Infra* note 324.
[314] *Ibid*, s 273.65(1).
[315] *Ibid*, s 273.65(2).

> **(d)** satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security

Additionally, this section also contains a catch-all provision, which stipulates that the Minister can add "any conditions that the Minister considers advisable to protect the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications".[316] In summary, this provision ensures that the CSE can only proceed where the Minister finds that the activity satisfies the safeguards illustrated above.

Furthermore, the *National Defence Act* also creates a safeguard mechanism within the executive branch. For instance, s. 273.63(1) of the *Act* states that the Governor in Council shall appoint a "supernumerary judge or a retired judge of a superior court" to be the Commissioner of the CSE for a term of no more than five years.[317] The Commissioner is responsible under the *National Defence Act* as follows. Firstly, the Commissioner is responsible for reviewing the "activities carried out under an authorization" to ensure that the CSE is authorized.[318] Secondly, the Commissioner must also create an annual report for the Minister of Defence.[319] Thirdly, the Commissioner is responsible for investigating complaints, if in the opinion of the Commissioner it is necessary to do so.[320] Should the Commissioner find a CSE activity to be in non-compliance with the law, the Commissioner is responsible for reporting this to the Minister of Defence and the Attorney General of Canada.[321]

---

[316] *Ibid*, s 273.65(5).
[317] *Ibid*, s 273.63(1).
[318] *Ibid*, s 273.65(8).
[319] *Ibid.*
[320] *Ibid*, s 273.63(2)(b).
[321] *Ibid*, s 273.63(2)(c).

In exercising his or her responsibilities, the Commissioner can use any powers present within the *Inquiries Act* to gather relevant information.[322] The powers granted to the Commissioner under the *Inquiries Act* provides the Commissioner with access to any of the CSE facilities, documents, and personnel.[323] In summary, the *National Defence Act* creates a Commissioner review process, which means the *Act* contains at least two oversight mechanisms.

Next, there will be a brief discussion as to how the *Privacy Act* creates certain oversight mechanism. As illustrated above, the *Privacy Act* is responsible for imposing certain obligations on federal departments and agencies, which includes the CSE. For instance, the *Privacy Act* restricts the way that personal information can be collected, used and disclosed.[324] The *Privacy Act* acts as an oversight mechanism in the sense that the Act stipulates the following. It states that personal information can only be collected if "it relates directly to an operating program or activity of the institution".[325] Therefore, the CSE can only collect information that is related to the program or an activity of the institution. By extension, the CSE is not authorized to collect information that has no nexus with the CSE program or activity. Secondly, the *Act* stipulates that the information collected will not be used without consent.[326] Additionally, should the information be used, where consent is granted, it shall only be used for "the purpose for which the information was obtained" or "for a use consistent with that purpose".[327] Thus, the CSE can only use the intercepted information for the purpose for which it was obtained. Thirdly, personal information may only be

[322] Canada, Office of the Privacy Commissioner of Canada, *Overview*, (Gatineau: OPC, 15 September 2015), online: <https://www.ocsec-bccst.gc.ca/en>.
[323] *Ibid.*
[324] *Privacy Act*, R.S.C., 1985, c. P-21.
[325] *Ibid*, s 4.
[326] *Ibid*, s 7.
[327] *Ibid*, s 7(a).

disclosed with consent, or if consent is unnecessary it must be the result of an exception within the *Act.*[328] In conclusion, the *Privacy Act* acts as an oversight mechanism in the sense that it regulate what information can be collected, how that information is to be retained, and if the information can be disclosed.

(b.) Oversight Bodies Within Executive Branch

The Canadian government has several oversight bodies present within the executive branch. For instance, the CSE is currently being overseen by the Office of the Communications Security Establishment Commissioner ("OCSEC"), the Office of the Privacy Commissioner ("OPC"), the Auditor General, the Office of the Information Commissioner ("OIC"). How each of these bodies act as an oversight mechanism will be discussed below.

Firstly, the role of the Office of the Communications Security Establishment Commissioner will be discussed. To recap, the Commissioner of the CSE has many responsibilities, such as the investigation of complaints and the review of CSE activities. In relation to the review process, the OCSEC has released a list of criteria that must be satisfied by the activity under review, which are as follows:[329]

> (1) it must meet the legal requirements set out in the *Charter of Rights and Freedoms*, *the National Defence Act*, and other relevant acts;
> (2) it must meet the ministerial requirements, which are set out in a ministerial authorization or directive;
> (3) the CSE must have appropriate policies and procedures in place that guide the CSE in meeting the legal and ministerial requirements.

[328] *Ibid*, s 8(1).
[329] Canada (Federal), Office of the Communications Security Establishment, *2017-2018 OCSEC Report*, (Gatineau: OPC, 15 September 2015), online: < https://www.ocsec-bccst.gc.ca/a280/ann-rpt-2017-2018-eng.pdf>.

Once the review process is complete, a classified report must be created and provided to the Minister that documents CSE activities.[330] In the report, it must describe to what extent the activity follows or deviates from the criteria listed above.[331] Additionally, the Commissioner can provide recommendations in the report that deal with how the CSE can correct problems or improve the privacy protection concerns stemming from the CSE activity or activities being reviewed.[332] Finally, in conducting a review the conclusions and findings must be "free of any interference by the CSE or any Minister".[333] Thus, the OCSEC in must act independently in conducting reviews, as they must free themselves from any bias. In relation to complaint investigations, the OCSEC is only responsible for investigating complaints if they find it is necessary to do so.[334]

Secondly, the CSE is also overseen by the Office of the Privacy Commissioner ("OPC"). To clarify, the OPC is responsible for overseeing the *Privacy Act* and *PIPEDA*. The CSE is subjected to the provisions found within the *Privacy Act*, as they are a government agency. Thus, by extension, the OPC can investigate and oversee CSE operations and activities in order to ensure compliance with the *Act*. For example, the *Privacy Act* states that information may only be collected if "it relates directly to an operating program or activity of the institution".[335] In response to such a complaint, the Privacy Commissioner can initiate an investigation under s. 29(1)(h)(i) of the *Privacy Act*. However, with respect to the CSE, the Privacy Commissioner's primary role is to ensure that the CSE is not abusing its authority by collecting and retaining information unlawfully. In exercising this role, the Privacy Commissioner has the authority to access any relevant

[330] *Ibid.*
[331] *Ibid.*
[332] *Ibid.*
[333] *Ibid.*
[334] *National Defence Act*, *supra* note 228, s 273.63(2)(b).
[335] *Supra* note 324, s 4.

information in the possession of the agency in question, subject to certain exceptions.[336] Furthermore, the Privacy Commissioner can enforce appearances by government official, administer oaths, and enter the premises of any government institution upon satisfying any security requirements.[337] Therefore, the Privacy Commissioner is another authority figure capable of overseeing the actions of the CSE when they engage in foreign intelligence operations.

Thirdly, at the executive branch level, the Auditor General acts as another oversight mechanism. The responsibility of the Auditor General's office ("AGO") is to assist in maintaining accountability within federal government departments by auditing the accounts of government agencies and operations.[338] The AGO is governed by the *Auditor General Act*. In conducting audits, the AGO's mission is to provide objective information, advice and assurance to Parliament. As part of their responsibilities, the AGO must make an annual report for the House of Commons.[339] In summary, the AGO is capable of acting as an oversight mechanism in the sense that they are a body that ensure that CSE is not inappropriately using funds for surveillance operations. Although, given that their role is financial oversight, this oversight mechanism is unlikely to impact a *GDPR* adequacy assessment.

Lastly, at the executive branch level, the Office of the Information Commissioner also act as an oversight authority where foreign surveillance is at issue. The Information Commissioner is an independent Ombudsman that reports directly to the House of Common and the Senate of

[336] *Ibid*, s 34(2).
[337] *Ibid*, s. 34(1).
[338] Office of the Auditor General, "The Role and Responsibilities of the Office of the Auditor General of Canada" (06 October 1998), online: *Office of the Auditor General* <http://www.oag-bvg.gc.ca/internet/English/meth_gde_e_10191.html>.
[339] *Auditor General Act*, R.S.C., 1985, c. A-17, s 7(1).

Canada.[340] The office was established in 1983 under the *Access to Information Act*.[341] Its purpose is to assist "individuals and organizations who believe that federal institutions have not respected their rights under the Act".[342] The *Access to Information Act* allows Canadian to request that the federal government disclose any information they have about the individual making the request.[343] However, the individual making the request must be a Canadian citizen or a Canadian resident.[344] Although, non-residents can simply use a Canadian proxy to exercise right under the *Act*.[345] In investigating complaints under the *Act*, the Information Commissioner has the same investigative powers as the Privacy Commissioner, which are illustrated above. Therefore, since the CSE is a government institution its activities are subject to the *Access to Information Act*. By extension, this means that the Information Commissioner is capable of investigating the CSE compliance with the *Act*. Thus, if the CSE is unlawfully retain the personal information of an individual, theoretically this Act can be used to review if theCSE are in non-compliance. However, the *Act* does have numerous exceptions; as a result, an individual might not be informed of all information possessed by government. For example, the federal government does not need to disclose information "which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities".[346] If an activity could not "reasonably" be expected to fall under one of these areas, then an individual should be able to gain access. Thus, if the CSE refuses to disclose information, the Information Commissioner could be

[340] Office of the Information Commissioner of Canada, "Who We Are" (19 December 2018), online: *Office of the Information Commissioner of Canada* <http://www.oic-ci.gc.ca/eng/abu-ans_who-we-are_qui-sommes-nous.aspx>.
[341] *Ibid.*
[342] *Ibid.*
[343] *Access to Information Act*, R.S.C., 1985, c. A-1, s 2(1).
[344] *Ibid*, s 4(1).
[345] Government of Canada, "Access to Information Act" (20 June 2019), online: *Government of Canada* <https://international.gc.ca/gac-amc/publications/atip-aiprp/index.aspx?lang=eng>.
[346] *Access to Information Act, supra* note 343, s 15(1).

used to ensure that the information is not being withheld unlawfully. In conclusion, the Information Commissioner can act as a foreign surveillance oversight mechanism.

(c.) Judicial Review

Judicial review is available under the *Privacy Act*, *PIPEDA*, and the *Access to Information Act*.[347] According to each of these statutes, after the Commissioner designated under the statute has completed his or her investigation, which stems from a refusal by government to disclose information within its possession, an individual can apply to the Federal Court to have the matter reviewed.[348] Therefore, in the event that a national security or surveillance agency is unwilling to disclose information, an individual can use the Federal Court to review the matter. Thus, in this circumstance the Federal Court can be used as an oversight mechanism. However, unlike the US *FISA* act Canada's *National Defence Act* is not subject to judicial review. Instead, as illustrated above, the CSE portion of the Act is reviewed by a Commissioner, which is usually a former judge, and the Minister of Defence.

(ii.) Personal Redress

In this section, there will be an overview of the Canadian personal redress mechanism available to non-citizens. First, there will be a description of the Canadian statutes that provide non-Canadian with personal redress, as it pertains to the use of personal data. There will also be a description of

[347] *Privacy Act*, *supra* note 324, s 41; *PIPEDA*, *supra* note 18, s 14(1); *Access to Information Act*, *supra* note 343, s 41.
[348] *Ibid.*

Canadian offices responsible for overseeing these statutes, as well as their roles and responsibilities. Afterwards, there will be a discussion that compares and contrasts the American approach to oversight and redress with the Canadian one. The purpose of that analysis will be to establish whether or not the Canadian approach will be found adequate under a *GDPR* assessment.

In Canada, there are two statutes that can be used by a non-Canadian to seek personal redress against government actions. The first is the *Privacy Act*, and the other one is the *Access to Information Act.*

As illustrated above, the *Privacy Act* governs how federal agencies and institutions can collect, use and retain personal information. Under this act, an individual can file a complaint with the federal Privacy Commissioner, the ombudsperson assigned to the Act.[349] According to the *Privacy Act*, nothing precludes a non- Canadian or non-resident from filing a complaint with the OPC.[350] As illustrated in the oversight section above, the Privacy Commissioner has a wide range of investigative tools at his or her disposal while conducting an investigation under the Act. If a complaint is well-founded, then the OPC shall report the findings along with any recommendations to the institution in possession of the personal information.[351] If the OPC finds it appropriate, the report will include a date that the offending agency must report back to the OPC, so that they may inform them of any action taken.[352] Furthermore, upon completion of the OPC's investigation, the Privacy Commissioner must also inform the complainant of the result of the OPC's

[349] *Supra* note 324, s 29(1).
[350] *Ibid*, s 29(2).
[351] *Ibid*, s 35(1).
[352] *Ibid* s 35(1)(b).

investigation.[353] Finally, if the complainant has been refused access to personal information lawfully requested to under the Act, and a complaint has been filed with the Privacy Commissioner, the complainant can "apply to the Federal Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Privacy Commissioner are reported to the complainant".[354]Thus, if a non-citizen wants to ensure that their personal information is being handled appropriately, then they can use this Act to achieve that end, as it create multiple personal redress avenues.

Additionally, a non-citizen or resident can also seek personal redress through the *Access to Information Act*. The purpose of the Act is to assist "individuals or organizations" who are of the opinion that a federal institution has not respected their rights under the Act.[355] Under the Act, a Canadian citizen or Canadian resident can request that the federal government disclose any information they have about the requesting individual.[356] Although, a non-Canadian individual can request a disclosure under the *Act*, if they use a Canadian citizen or resident as a proxy. The ombudsman person responsible for overseeing the Act is the Information Commissioner.[357] Under the *Act*, the Information Commissioner is capable of investigating complaints of non-compliance under the Act.[358] In conducting investigations, the Information Commissioner has the same investigative powers as the Privacy Commissioner, which are illustrated in the oversight section above. Upon completion of investigation, the Information Commissioner must inform the complainant of the results of the investigation.[359] Additionally, if the Commissioner finds that the

[353] *Ibid*, s 35(2).
[354] *Ibid*, s 41.
[355] *Ibid.*
[356] *Supra* note 343, s 4(1).
[357] *Ibid*, s 30(1).
[358] *Ibid.*
[359] *Ibid*, s 37(2).

complaint is well-founded, the Commissioner will issue a report to the offending agency that shows their findings and recommendation.[360] Where appropriate the report will contain a time period within which the offending agency must report back to the Commissioner of any action taken.[361] Should an agency refuse to provide access to a record requested under the Act, and a complaint has been filed with the Information Commissioner, that person can "apply to the Federal Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Information Commissioner are reported to the complainant".[362] However, the *Access to Information Act* does contain several exceptions, which can justify non-disclosure by federal agency or institution. For instance, a federal agency or institution does not have to disclose information "which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities".[363] In summary, the *Access to Information Act* does provide non-Canadian's with avenues to seek personal redress, if there information is not being held under one of the Act's exceptions.

In conclusion, both the *Privacy Act and the Access to Information Act* include personal redress mechanisms. Both Acts enable individuals to file complaints with an ombudsman. Additionally, the ombudsman person is then responsible for investigating the complaint, as well as informing the complainant of the results of their investigation. Both Acts provide their respective ombudsman person with a wide range of investigative tools, for instance they can search the premises of any federal agency. Finally, the Acts provide a non-citizen with access to the Federal Court if judicial

[360] *Ibid*, s 37(1).
[361] *Ibid*, s 37(1)(b).
[362] *Ibid*, s 41.
[363] *Ibid*, s 15(1).

review is justified. Thus, in summary the Canadian government has provided individuals with several personal redress mechanisms.

3. Comparative Analysis: Canadian vs. American Approach to Oversight and Personal Redress

(i.) Oversight in the Executive Branch

In this section, there will be a comparative analysis that addresses the similarities and differences that exist between the Canadian and American oversight mechanisms at the executive branch level. The objective is to establish whether or not the EU Commission will find the Canadian approach sufficient under the *GDPR*. This analysis will be used to support a conclusion about an EU adequacy decision.

As illustrated above, the Canadian government provides oversight at the executive branch level through the OCSEC, the Privacy Commissioner's Office and through the Information Commissioner's Office. However, due to the fact that the Privacy and Information Commissioner's roles are specific to personal redress, they will be discussed more in depth during the personal redress section below. Thus, this analysis will focus primarily on the oversight provided by OCSEC, which will be compared to the US executive branch oversight mechanisms.

In the US, at the executive branch level, oversight is provided by Inspectors-General, the Privacy and Civil Liberties Board, civil liberties or privacy officers, the Privacy and Civil Liberties Board, and the President's Intelligence Oversight Board. The role of each of these bodies will be compared and contrasted with OCSEC below.

The Inspector-General is an executive body responsible for overseeing the activities of each intelligence agency.[364] For example, the Inspector-General is authorized to evaluate an intelligence agency's compliance with targeting and minimization procedures.[365] Additionally, the Inspector-General can assist the Privacy Shield Ombudsperson in assessing compatibility of intelligence surveillance with U.S. law.[366] Furthermore, the Inspector-General is capable of investigating complaints against the intelligence agency, such as abuse of authority.[367] In conducting an investigation, the Inspectors-General have access to audits, documents, reviews, and any other relevant material. Once an investigation is completed, the Inspectors-General can issue a non-binding compliance recommendation for corrective action, which are placed in a report and are made available to the public and Congress.

In comparison, the OCSEC, like the Inspectors-General, is also responsible for overseeing intelligence activities. For instance, the CSE Commissioner's mandate is "to review activities of CSE – which includes foreign signals intelligence and information technology (IT) security activities to support the Government of Canada – to determine whether they comply with the law".[368] Therefore, both executive bodies play a similar role in ensuring that intelligence agencies remain compliant with the law. Additionally, the CSE Commissioner has powers that are comparable to those afforded to the Inspectors-General. For example, the Commissioner has all the powers present under Part II of the *Inquiries Act*, which includes the authority to gains access

[364] *US Adequacy Decision*, *supra* note 197: ODNI Representations (Annex VI), p. 7. See e.g. NSA, PPD-28 Section 4 Procedures, 12 January 2015, Sec. 8.1; CIA, Signals Intelligence Activities, p. 7 (Responsibilities).
[365] *Ibid* at para 103.
[366] *Ibid* at para 120.
[367] *US Adequacy Decision*, *supra* note 199.
[368] *2017-18 OCSEC Report*, *supra* note 329.

to a government department's premises, examine documents and records, require an appearance by an individual of interest, and administer oaths.[369] As a result, the CSE Commissioner has the same investigative tools as do the U.S. Inspectors-General. In conducting an investigation, the CSE Commissioner must ensure that a list of criteria is being met by the CSE, which includes compliance with the *Charter*, the *National Defence Act*, and any other relevant Act.[370] This further illustrates that, like the Inspector-General's mandate, the CSE Commissioner's primary role is to ensure compliance with Canadian law. Once an investigation is complete, the CSE Commissioner must create a classified report, which is issued to the Minister of Defence.[371] In this report, the CSE Commissioner can provide recommendations as to how the CSE can improve. The Commissioner is also responsible for creating an annual report, which details if the CSE has been compliant with the law, and follows up on past recommendations.[372] This report is made available to the public. Thus, both the CSE Commissioner and the Inspector Generals promote compliance and oversight by issuing reports, and by making recommendations. Additionally, both bodies make their reports available to Parliament and the public. Finally, both the OCSEC and the Inspector Generals are independent bodies. Therefore, this means that they are not subjected to bias by the agencies that they investigate. In conclusion, the OCSEC has the same responsibilities and powers as does the US Inspector General.

The US Privacy and Civil Liberties Board is an independent agency responsible for overseeing the implementation and use of counterterrorism policies.[373] In exercising this role, the Board tries to

[369] *Inquiries Act* R.S.C., 1985, c. I-11, s. 7.
[370] *2017-18 OCSEC Report*, *supra* note 329.
[371] *Ibid.*
[372] *National Defence Act*, *supra* note 228, s 273.63(1).
[373] *US Adequacy Decision*, *supra* note 199 at para 98.

ensure that American privacy and civil liberties are addressed within these policies.[374] In conducting a review of an intelligence agency's actions, the Board can investigate records, documents, reports, and any other relevant material.[375] The Board can also receive reports from all the civil liberty and privacy officers.[376] In response, the Board can provide these officers with recommendations. Moreover, the Board can also provide Congressional committees and the President with a Report.[377] Thus, the Board acts as an oversight mechanism for both counterterrorism policy and the civil liberties or privacy officers.

By comparison, the CSE Commissioner is also tasked with ensuring that the CSE policies adequately respect Canadian privacy and civil liberty laws. For example, OCSEC reports stipulate that the CSE Commissioner expects the "CSE to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians".[378] Additionally, the CSE Commissioner expects the CSE to have "an effective compliance validation framework to ensure the integrity of operational activities is maintained", and which appropriately protects "the privacy of Canadians". Therefore, like the US Privacy and Civil Liberties Board, the CSE Commissioner is responsible for overseeing counterterrorism policies. Furthermore, like the Board the CSE Commissioner also has similar investigative powers. Additionally, should the CSE Commissioner disagree with how certain policies are being implemented, the Commissioner can provide the Minister of Defense with a classified report that illustrates the Commissioner's perspective. The Commissioner can

[374] *Ibid.*
[375] *Ibid.*
[376] *Ibid.*
[377] *Ibid.*
[378] *2017-18 OCSEC Report*, *supra* note 329.

also provide recommendation as to how the policy should change, and can follow up on if the recommendation has been implemented. Therefore, both bodies can influence counterterrorism policy through reports and recommendations. In conclusion, the CSE Commissioner has the same powers and responsibilities as the U.S. Privacy and Civil Liberties Board does.

In conclusion, based on the comparisons listed above, the Canadian oversight at the executive branch is essentially equivalent to the U.S.

(ii.) Personal Redress and Statutory Review

In this section, the Canadian and American approach to personal redress will be compared. Both countries have statutory mechanisms and independent Ombudsman persons which provide personal redress to citizens and non-citizens. These approaches will be compared and contrasted with each other in order to assess whether the EU Commission will find the Canadian approach adequate under the *GDPR*.

(a.) Statutory Personal Redress

As illustrated above, the *Foreign Intelligence Surveillance Act* ("*FISA*") allows non-U.S. citizens to challenge U.S. surveillance in several ways. For one, a non-citizen can bring forward a civil action for monetary damages if they can establish that the US unlawfully and willfully used or disclosed their personal information.[379] Additionally, a non-citizen can challenge the use of the

[379] 18 U.S.C. § 2712.

information in judicial or administrative hearings.[380] Finally, *FISA* does also allow the US government to be sued personally for misuse or mistaken collection of personal information during surveillance.[381]

The Canadian equivalent to *FISA* is the *National Defence Act* ("*NDA*"). Under the *NDA*, if information is lawfully gathered under s. 273.65 of the Act (Ministerial authorization section) then the Crown is shielded from any liability.[382] However, should the intercepted communication fall outside of the ministerial authority there is an argument to be made that this triggers Crown liability under s. 18 of the *Crown Liability and Proceedings Act*.[383] Thus, similar to *FISA*, the *NDA* does appear to indicate that the Crown can be held liable for unlawful interception and use of a non-Canadian's personal information. Notwithstanding this similarity, the *NDA* does differ from *FISA* in the sense that the *Act* is silent as to whether or not a non-Canadian can challenge the use of intercepted communication during judicial or administrative proceedings. However, this information likely can be challenged through the *Privacy* and *Access to Information Act* judicial review process, or through the *Canada Evidence Act* rules regarding admissibility of evidence. Therefore, the language under the *NDA* is substantially similar to that of the *FISA* with regards to personal redress. As a result, the EU commission would likely find that these statutes are similar in terms of personal redress.

[380] 50 U.S.C. § 1806.
[381] 50 U.S.C. § 1810.
[382] *Supra* note 228, s 273.70.
[383] *Crown Liability and Proceedings Act*, R.S.C., 1985, c. C-50, s 18.

The *Administrative Procedure Act* is the next U.S. statutory ground for personal redress identified in the EU-US Privacy Shield adequacy report.[384] Under this *Act*, "any person suffering legal wrong because of any agency action, or adversely affected or aggrieved by such action within the meaning of any relevant statute, shall be entitled to judicial review".[385] If the reviewing court finds that the action was "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law", it can pronounce the action unlawful and order that it be set aside [386]

By comparison, Canada has several statutes that afford non- citizens similar protection. For instance, both the *Privacy Act* and the *Access to Information Act* allow affected individual to pursue judicial review where agency action is being criticized. However, as illustrated above, certain preliminary steps must be undertaken prior to exercising this option, such as an investigation by the appropriate commissioner must be undertaken. If the reviewing court finds the action unlawful, the Court can it set aside. Thus, the protections afforded by the *Administrative Procedure Act* can also be found in numerous Canadian statutes.

Furthermore, the EU-US Privacy Shield adequacy decision also discussed the US *Freedom of Information Act* when it evaluated their personal redress mechanisms. Under the *Act*, non-U.S. citizens can ensure that the U.S. government only possesses information that they are lawfully allowed to possess. Moreover, under the *Act*, individuals can also determine if the information is being used lawfully. However, the *Act* is limited in the sense that there a numerous exceptions to

[384] *Administrative Procedure Act*, Pub.L. 79–404, 60 Stat. 237.
[385] *Ibid*, s 10(2)(a).
[386] 5 U.S.C. § 706(2)(A).

disclosure, such as a restriction on access to information that is classified based on national security grounds.[387]

The Canadian government has also passed a similar statute referred to as the *Access to Information Act*. As illustrated above, the purpose of the *Act* is to provide individuals with access to the information that the Canadian government has with respect to them, and to enable individuals to challenge any unlawful possession of their information. Therefore, the Canadian *Access to Information Act* is substantially similar to the US *Freedom of Information Act* as both statutes provide individuals with similar rights. Although, these Acts do differ in the sense that the Canadian statute does allow individuals to bring their grievance forward under judicial review, whereas the U.S. statute does not. Thus, not only does the Canadian statute provide equal amounts of protection, it also arguably provides more through its judicial review provision.

In conclusion, the American statutory personal redress mechanisms each have equivalent or superior Canadian counterpart. As a result, at this point of the analysis it would appear as though the Canadian approach to personal redress would be found adequate under the *GDPR*. However, the EU-US Privacy Shield adequacy decision made it clear that the creation of an independent Ombudsman Person was the true reason for its adequacy under personal redress. Therefore, below the analysis will determine whether or not there is a Canadian equivalent to the EU-US Privacy Shield Ombudsman Person described in the report. This portion of the analysis will be central to an adequacy determination.

[387] 5 U.S.C. § 552.

(b.) Independent Ombudsman Person

As illustrated above, the EU Commission had several concerns that resulted in the EU-US Privacy Shield Ombudsman Person being created. The EU Commission was of the opinion that there were situations that existed where EU citizens could not get any redress, such as when Executive Order 12333 is used.[388] Moreover, they found that the even where the U.S. statutes provided grounds for redress, their grounds were limited and standing was an issue. In order to alleviate these concerns, the Ombudsperson is charged with ensuring that complaints are properly investigated, and that American agencies have complied with the law.[389]

If the Ombudsperson finds that U.S. laws have been violated, the Ombudsperson must provide confirmation that there has been non-compliance and that it has been remedied.[390] In order to determine compliance, the Ombudsperson is authorized to use independent oversight bodies with investigative powers. For example, the Ombudsperson is authorized to use the Inspectors-General or the PCLOB for assistance.[391] Where non-compliance with U.S. laws have been identified, the non-compliance must be remedied so that the Ombudsperson can communicate to the affected party that the issue has been remedied.[392]

Finally, in the report the EU Commission emphasized the need for this Ombudsperson to be fully informed and an independent body. For instance, they emphasized that the Ombudsman person

[388] *US Adequacy Decision*, *supra* note 199 at para 115.
[389] *Ibid* at para 117.
[390] *Ibid.*
[391] *Ibid.*
[392] *Ibid* at para 120.

must not be instructed by the intelligence community, as this is necessary to avoid bias and coercion.[393] Additionally, the emphasis on fully informed is necessary as the body can only be effective if the Ombudsman person has complete access to all necessary information.

If Canada is to be found adequate in terms of personal redress, then it will need to establish that similar protections to those provided by the EU-US Privacy Shield Ombudsman Person exist in Canada. The Canadian government might argue that such an Ombudsman Person already exists. For instance, they would likely point to the Commissioners under the *Privacy Act* and the *Access to Information Act*, respectively, as being the Canadian equivalents.

Under both Acts, the Commissioners are responsible for receiving complaints about the possession or handling of their personal information. As illustrated above, these Commissioners have investigative powers provided to them via the *Enquiries Act*. Therefore, the Commissioners are each capable of independently investigating any complaint permitted under their respective statutes. Nothing under these Acts prevents the Commissioners from using other independent bodies for assistance. Furthermore, these bodies are independent from the intelligence community. As a result, they should theoretically be free from coercion and bias. Furthermore, the *Privacy Act* and *Access to Information Act* both require that their Commissioners report back to the complainant the result of their investigation. Finally, should the grievance not be remedied through the Commissioner's formal investigation, each statute authorizes the affected party to pursue the action through judicial review before the Federal Court.

[393] *Ibid* at para 121.

Therefore, based on the presence of these two Ombudsman persons, the EU Commission should find that Canada has an adequate personal redress mechanism. The Canadian Ombudsman persons already engage in a similar review and reporting process. Secondly, they are independent authorities that are fully informed, which satisfies that *GDPR* requirement.

(c.) Conclusion

In conclusion, if the EU Commission is willing to accept the US's approach to personal redress then Canada is likely well-suited to obtain an adequacy finding here as well. As illustrated above, the personal redress mechanism afforded by *FISA* is essentially equivalent to that offered by the *NDA*. Additionally, the US's *Administrative Procedure Act* provides the same protections as does the Canadian *Privacy Act* and *Access to Information Act*. In fact, the Canadian Acts provide further protection as they allow for judicial review. Further, both countries contain substantially similar access to information statutes. Finally, the Canadian government likely has strong grounds to argue that we already have an EU-US Privacy Shield Ombudsman Person equivalent in the form of the Commissioners described above. Therefore, on this basis the EU Commission should accept that Canada's personal redress mechanisms are adequate. However, if they do not accept Canada's current structure, the Canadian Government and the Commission could always work out a new position to fill the gaps.

(iii.) Conclusion

Based on the analysis above, the Canadian approach to both enforcement at the executive branch and to personal redress is essentially equivalent to the US approach. As a result, the EU Commission will likely find that the Canadian approach to oversight and redress is "essentially equivalent" to the *GDPR*. This conclusion is supported by the fact that the EU Commission found the US approach in these areas essentially equivalent, using the *Schrems* principles. Therefore, since the Canadian approach is essentially equivalent to the American approach it is also likely to satisfy the EU Commission's equivalency test.

Conclusion

The *GDPR* has ushered in a new era of privacy protection and has brought with it a new standard of data protection. Under the previous European privacy-protection model, Canada's data protection regime was found to be adequate. However, the standard of what is "adequate" has changed following the European Court of Justice's decision in *Schrems*. In this decision, the Court decided to look at privacy protection from a more holistic perspective by taking into account factors such as national security and oversight mechanisms. This holistic approach was implemented into Article 45(2)(a)-(c) of the *GDPR*. This article illustrates the test that the EU Commission utilizes in determining whether a "third country" is deemed "adequate" under the *GDPR*. The test has the EU Commission assess if the third country's privacy legislation, oversight mechanisms and national security laws are adequate. There are additional elements that Article 45 considers. However, this paper focused on these three factors as they are likely to be given the most weight by the EU Commission.

This paper seeks to answer if Canada's privacy protection framework will be found adequate under an assessment by the EU Commission. Each component of the Article 45 test discussed above were addresses to answer the question of adequacy.

In Part I, the issue of whether Canada's federal privacy legislation would be deemed adequate under Article 45 was addressed. The analysis under this Part looked at the key provision found within the *GDPR* and compared them to the comparable provisions found within *PIPEDA*. The following data protection provisions were evaluated: consent, right of access, data protection by

design, the right to be forgotten, data portability and data breach reporting. Each of these concepts was evaluated individually. However, the final conclusion on *PIPEDA*'s adequacy looked at these concepts holistically and took into account the novel nature of some the *GDPR*'s new provisions.

Based on the analysis, *PIPEDA* contains adequate consent, right of access and data breach reporting provisions. However, there are slight differences between the *GDPR* and *PIPEDA* in two of these concepts. For example, the *GDPR* has a similar consent model to *PIPEDA*, as both focus on the data controller's ability to demonstrate consent, but the *GDPR* provides greater protection to minors. Additionally, the *GDPR*'s right to access provision is slightly more comprehensive than *PIPEDA*'s, as the former requires that data controller's provide access to information such as the source of the data being held and data subject can request that information be erased. Notwithstanding these differences, the EU Commission would like find that *PIPEDA* "adequately" addresses the areas of consent, right of access and data breach reporting.

Part I does highlight a few areas where *PIPEDA* does not have an equivalent provision to the *GDPR*. These areas are privacy by design, data portability and the right to be forgotten. All three of these concepts are absent from *PIPEDA*. Some have argued that there is a right to be forgotten within *PIPEDA*. As illustrated by the analysis in Part I, the Office of the Privacy Commissioner believes that that *PIPEDA* has a right to be forgotten, as they believe indexing is a commercial activity and the OPC is of the opinion that search engines collect, use and disclose personal information. However, even if these sections are not addressed by *PIPEDA* this is likely not fatal to an adequacy finding as the EU Supervisor told the Canadian Parliament that they should "not

focus too much on the novelties in the GDPR, such as design, default, and portability" [394]. Therefore, these factors were considered in the determination of "adequacy", but they were not weighed as heavily.

To summarize the conclusion in Part I, *PIPEDA* is in a grey area when it comes to adequacy. The legislation is outdated and has not been amended to reflect a changing privacy landscape. Although the statute does address core concepts in an "essentially equivalent" manner, at least two out of three of these provisions are outdated. For instance, the *PIPEDA* consent model does not adequately protect minors and the right to access section is not as robust as the *GDPR*. Additionally, *PIPEDA* also finds itself in a grey area because it has failed to keep up with modern privacy protection concepts, such as privacy by design and data portability. The EU Commission might take issue with the fact that Canada has not updated their privacy legislation in non-novel areas. The outdated nature of *PIPEDA* in addition to the absence of novel concepts might be enough for a negative adequacy finding. However, because the Canadian Parliament was told "not focus too much on the novelties in the GDPR, such as design, default, and portability" and because the standard is "essential equivalence" *PIPEDA* is likely going to be found adequate [395].

In Part II, an analysis was undertaken to determine if the enforcement of *PIPEDA* would be considered adequate under the *GDPR*. This was done by comparing the *GDPR* enforcement mechanisms with those used to enforce *PIPEDA*. This Part illustrates the following points. The *GDPR* and *PIPEDA* use different model for enforcement. For example, the *GDPR* uses an order-making model whereas *PIPEDA* uses ombudsman model. As a result, supervisory authorities can

[394] ETHI, *supra* note 111.
[395] *Ibid.*

issue orders to force compliance with its Articles, while the Privacy Commissioner can only issue compliance agreements. These agreements can only be enforced by Canada's Federal Court. Secondly, the *GDPR* supervisory authorities can issue sanctions, whereas the Canadian Privacy Commissioner does not have authority to do so as the Federal Court has this power. Despite these differences, Part II concludes that the enforcement of Canadian privacy legislation will likely still be found adequate as Canada does implement the same enforcement mechanism. Canada simply uses two different enforcement bodies instead of one. Although this might be less efficient, it is still "essentially equivalent".

Part III analyzed how the Canadian government accesses, uses and stores the personal data of EU citizens for national security purposes. Additionally, this section also evaluates the legal protections available to EU citizens under the Canada privacy protection framework.

In this Part, there was a conclusion that the Canadian approach to EU information access, storage and use was comparable to the American Approach. For instance, Canada *National Defence Act* contains provisions that restrict collection of information in way that is similar to the requirements under Presidential Policy Directive 28. Additionally, both restrict access to foreign intelligence information by limiting access to qualified and trained personnel. Moreover, both countries restrict how long information can be held. For instance, both the PPD-28 and Canada's *National Defence Act* contain language that limit the retention of personal information. Therefore, based on the analysis in Part III, the EU Commission will likely find that Canada's use, access and retention of foreign intelligence is adequate under the *GDPR*.

In considering the legal protections available to EU citizens, a comparative analysis was conducted. The Canadian approach was compared to the American approach, as the American approach in this area was accepted by the EU Commission as being adequate in 2016. The Canadian approach was determined under the analysis to be adequate for several reasons. First, at the executive branch level, the OSEC, the Privacy Commissioner and the Information Commissioner have the same enforcement and oversight powers as their American counterparts. Additionally, from statutory and personal-redress standpoint, the Canadian legislation contained equivalent personal and statutory redress measures, For example, both the *Privacy Act* and *Access to Information Act* allow EU citizens to file complaints with an ombudsman person and that person is responsible for investigating the complaint and for reporting back to the complainant. This approach is essentially equivalent to the American approach, where they have an ombudsman person assigned to do the same things.

Therefore, based on the reasons listed above and in Part III itself, there was a finding that the Canadian approach to national security would likely adequate by the EU Commission. Additionally, the legal protection present with Canadian legislation are also likely to be found adequate.

In conclusion, based on the analysis in all three Parts it is likely that the EU Commission will find that the Canadian privacy framework is adequate. As illustrated above, the outdated nature of *PIPEDA* is a concern. However, Canada's approach to national security, legal protection and

oversight will likely to outweigh any concerns the EU Commission might have with regards to *PIPEDA* shortcomings.

Bibliography

Legislation

Federal Statute

Access to Information Act, R.S.C., 1985, c. A-1.

Auditor General Act, R.S.C., 1985, c. A-17.

Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23.

Crown Liability and Proceedings Act, R.S.C., 1985, c. C-50.

Digital Privacy Act, SC 2015, c 32.

Inquiries Act R.S.C.**,** 1985, c. I-11.

National Defence Act, R.S.C., 1985, c. N-5

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

Privacy Act, R.S.C., 1985, c. P-21.

Security of Information Act, R.S.C., 1985, c. O-5.

Europe

Charte sur la publicité ciblée et la protection des internautes [Code of Good Practice on Targeted Advertising and the Protection of Internet Users] France 2010, online: *UFMD* <https://uniondesmarques.fr/l/library/download/5472/20100929_charte_pub_ciblee_protection_internaute.pdf>.

Data Protection Directive, European Union, 24 October 1995, (13 December 1995).

EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*) [2016] OJ, L 119/1 p. 1-88.

United States

Administrative Procedure Act, 5 U.S.C. § 706(2)(A).

Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub L No 95–511, 92 Stat. 1783.

Inspector General Act of 1978, §§ 4(5), 5.

The Intelligence Authorization Act.

42 U.S.C. § 2000 ee-1.

50 U.S.C. § 413(a)(1).

50 U.S.C. § 413(b).

18 U.S.C. § 2712.

5 U.S.C. § 702.

12 U.S.C. § 3417.

USA Freedom Act of 2015, Pub. L. No 114-23, § 602(a).

Freedom of Information Act, 5 U.S.C. § 552.

Jurisprudence

Canada

A.T. v. Globe24h.com, [2017] 4 FCR 310, 2017 FC 114 (CanLII).

State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada, 2010 FC 736 (CanLII).

Europe

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield *(notified under document C (2016) 4176)*.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Google Spain v Gonzalez) (2014), ECR C-131-12.

Government Documents

Executive Order

United States, Office of the Director of National Intelligence ("ODNI"), *Executive Order 12333* (Executive Order), online: *ODNI* < https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333>.

Hansard

ETHI, Evidence, 1st Session, 42nd Parliament, 16 February 2017, 1245 & 1250.

ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1555 (Chantal Bernier).

ETHI, Evidence, 1st Session, 42nd Parliament, 16 February 2017, 1545 (Daniel Therrien).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0855 (Daniel Therrien).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1555 (Dennis Hogarth, Vice-President, Consumers Council of Canada).

ETHI, Evidence, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Dr. Eloise Gratton).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Éloïse Gratton).

ETHI, Evidence, 1st Session, 42nd Parliament, 13 June 2017, 1240 (Giovanni Buttarelli, Supervisor, European Data Control Supervisor).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Linda Routledge).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1635 (Michael Karanicolas).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1530 and 1605 (Michael Karanicolas).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1535 (Owen Charters).

ETHI, Evidence, 1st Session, 42nd Parliament, 13 June 2017, (Raj Saini, Liberal Member of Parliament).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Robert Dickson).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1640 (Suzanne Morin).

ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1545 (Teresa Scassa).

Opinions

Office of the Privacy Commissioner, *Draft OPC Position on Online Reputation*, De-indexing and Source Takedowns (26 January 2018), online: *Office of the Privacy Commissioner* < https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/>.

Policies

Office of the Privacy Commissioner, *2018-19 Departmental Plan: Office of the Privacy Commissioner of Canada*, Spending and Human Resources (16 April 2018), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2018-2019/dp_2018-19/#heading-0-4-1>.

Safe Harbor Privacy Principles, United States, (26 July 2000 | EU recognizes "Safe Harbor Privacy Principles" issued by Department of Commerce).

United States, Office of the Director of National Intelligence ("ODNI"), *Presidential Policy Directive 28 ("PPD-28* (Presidential Directive), online: *ODNI* < https://www.dni.gov/index.php/ic-legal-reference-book/presidential-policy-directive-28>.

Public Information

Canada (Federal), Office of the Communications Security Establishment, *2017-2018 OCSEC Report*, (Gatineau: OPC, 15 September 2015), online: < https://www.ocsec-bccst.gc.ca/a280/ann-rpt-2017-2018-eng.pdf>.

Canada, Office of the Privacy Commissioner of Canada, *Overview*, (Gatineau: OPC, 15 September 2015), online: <https://www.ocsec-bccst.gc.ca/en>.

Communications and Security Establishment, "Foreign Signals Intelligence" (01 August 2019), online: *Government of Canada* <https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement>.

Government of Canada, "Access to Information Act" (20 June 2019), online: *Government of Canada* <https://international.gc.ca/gac-amc/publications/atip-aiprp/index.aspx?lang=eng>.

Government of Canada, "Foreign signals intelligence" (01 August 2018), online: *Government of Canada* < https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement>.

Government of Canada, "*SIGINT* Security (CSE)", online: *Government of Canada* <https://www.cse-cst.gc.ca/en/learning-formation/area-region/sigint-security>.

US Senate Select Committee on Intelligence, "Overview of the Senate Select Committee on Intelligence Responsibilities and Activities" (10 October 2019), online: *US Senate* <https://www.intelligence.senate.gov/about>.

Office of the Auditor General, "The Role and Responsibilities of the Office of the Auditor General of Canada" (06 October 1998), online: *Office of the Auditor General* <http://www.oag-bvg.gc.ca/internet/English/meth_gde_e_10191.html>.

Office of the Information Commissioner of Canada, "Who We Are" (19 December 2018), online: *Office of the*

Reports

House of Commons, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act***,** Report of the Standing Committee on Access to Information, Privacy and Ethics, 42nd PARLIAMENT, 1st SESSION (February 2018), online: <http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12>.

Michael Karanicolas of the Centre for Law and Democracy (CLD): (2016 Report).

Office of the Privacy Commissioner, *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*, Children and Youth (21 September 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1-3-3>.

Office of the Privacy Commissioner, *2017-18 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*, Reputation (27 September 2018), online: *Office of the Privacy Commissioner* < https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/>.

Office of the Privacy Commissioner, *Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA: PIPEDA Report of Findings #2015-002*, (06 June 2015), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-002/>.

PCLOB, Sec. 215 Report.

PLCOB, Sec. 702 Report.

Representations

Official Journal of the European Union, ODNI Representations (Annex VI) p. 3 (US adequacy report), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN#ntr63-L_2016207EN.01000101-E0063>.

ODNI Representations (Annex VI), p. 6 (with reference to Intelligence Community Directive 204).

Secondary Sources

Andrea Gonsalves, "Privacy Commissioner's Draft Report on a "Right to be De-Indexed" is Cause for Concern (26 March 2018), online (blog): *Andrea Gonsalves* <https://cfe.ryerson.ca/blog/2018/03/privacy-commissioners-draft-report-right-be-de-indexed-cause-concern>.

Allen Mendelsohn, "Forget the Right to be Forgotten (For Now)" (28 February 2017), online (blog): *Allen Mendelsohn* <http://allenmendelsohn.com/2017/02/forget-the-right-to-be-forgotten-in-canada-for-now/>.

Ana Cavoukian, "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", online (blog): *Ana Cavoukian* <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf>.

Article 29 Data Protection Working Party, "17/EN WP 254: Adequacy Referential (updated)" (28 November 2017), online: *ec.europa.eu* < http://webcache.googleusercontent.com/search?q=cache:ymgOKk-scioJ:ec.europa.eu/newsroom/just/document.cfm%3Fdoc_id%3D48827+&cd=1&hl=en&ct=clnk&gl=ca&client=safari>.

Aysem Vanberg, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?" (2017) 8:1 Eur J Law 1–22.

Barry Bookman, "PIPEDA's global extra-territorial jurisdiction: A.T. v. Globe24h.com" (3 February 2017), online (blog): *Barry Bookman* <https://www.mccarthy.ca/en/insights/blogs/cyberlex/pipedas-global-extra-territorial-jurisdiction-v-globe24hcom>.

Carmela Troncoso, "Engineering Privacy By Design" (2017), online: <https://summerschool-croatia.cs.ru.nl/2017/slides/Engineering%20privacy%20by%20design.pdf>.

Colin Freeze, "CSEC won't say how long it keeps Canadians' private data", *Globe and Mail* (04 August 2014), <www.globeandmail.com>.

David Fraser, "Did the Canadian Federal Court take the first step to a "right to be forgotten" with a global take-down order?" (7 February 2017), online (blog): *David Fraser* <https://canliiconnects.org/en/commentaries/44665>.

David Krebs, "Implementing Privacy By Design" (5 November 2018), online (blog): *David Krebs* <https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/implementing-privacy-by-design/>.

European Data Protection Supervisor (EDPS), "Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability, Opinion 7/2015" (19 November 2015) at 13, online (pdf): *Europe Data Protection Supervisor* <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>.

European Union Agency for Network and Information Security, "Privacy and Data Protection by Design – from policy to engineering" (2014), online (pdf): *ENISA* < https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

Google, "Transparency Report: Requests to delist content under European privacy law" (24 September 2019), online: *Google.ca* < https://transparencyreport.google.com/eu-privacy/overview?hl=en>.

Inge Graef et al., "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" (2018) 19:6 German L.J. 1359 1359-1398 at 1359-60.

Ira Rubenstein & Nathaniel Good, “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents” (2013) 28:1333 BTLJ at 1408, online: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2007&context=btlj>.

Jennifer McClennan & Vadim Schick, "O, Privacy: Canada's Importance in the Development of the International Data Privacy Regime" (2007) 38 Geo J Intl L: 669–693 at 671.

John Choudhari, “Cataloging GDPR complaints since May 25” (25 June 2018), online (blog): *John Choudhari* <https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/>.

Ken Clark, “Google Fails to Amend Canadian De-indexing Injunction Despite California Court Order” (23 April 2018), online (blog): *Ken Clark* <https://www.lexology.com/library/detail.aspx?g=baf6ee19-f1dc-4c92-b094-53ef700a4eb5>.

Laura Kayali, “France hits Google with €50 million fine for GDPR violation” (19 April 2019), online: *Politico* <https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/>.

Michel Finck, “Google v CNIL: Defining the Territorial Scope of European Data Protection Law” (16 November 2018), online: *University of Oxford: Faculty of Law* < https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law>.

Michael Geist, “Did a Canadian Court Just Establish a New Right to be Forgotten?" (7 February 2017), online (blog): *Michael Geist* <http://www.michaelgeist.ca/2017/02/did-a-canadian-court-just-establish-a-new-right-to-be-forgotten/>.

OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, online: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

Paul De Hert et al., “The right to data portability in the GDPR: Towards user-centric interoperability of digital services” (2018) Computer L and Sec Review 193-203 at 194.

Paul Quinn, “Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?” (2018) 18:2 Global Jurist 81-97 at 81.

Robert Madge, “GDPR: data portability is a false promise” (4 July 2017), online (blog): *Medium* <https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629>.

Seda Gurses et al., “Engineering privacy by design” Paper delivered at the Conference on Computers, Privacy & Data Protection, CPDP 2011 (2011) [unpublished], online: <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf>.

Teresa Scassa, “OPC Report on Online Reputation Misses the Mark on the Application of PIPEDA to Search Engines” (31 January 2018), online (blog): *Teresa Scassa* <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=270:opc-report-on-online-reputation-misses-the-mark-on-the-application-of-pipeda-to-search-engines&Itemid=80>.

The Canadian Press, “Privacy czar asks Federal Court to settle 'right to be forgotten' issue” (10 October 2018), online (blog): *BNN Bloomberg* < https://www.bnnbloomberg.ca/privacy-czar-asks-federal-court-to-settle-right-to-be-forgotten-issue-1.1150495>.