UiO : Faculty of Law
University of Oslo

Tracing the Inadequacies of Canadian Federal Privacy Law

An evaluation of the law relating to contact tracing applications, and how the EU may provide insight for revision.

Candidate number: 8010

Submission deadline: 1 December 2020

Number of words: 17,477 words

Acknowledgements

Over the course of crafting this thesis, I received an incredible amount of invaluable support and guidance, without which, I would have been unable complete this paper.

I would first like to sincerely thank Dr. Barbara von Tigerstrom, for agreeing to supervise this thesis. I deeply appreciate you sharing your time, knowledge, advice, and feedback, all of which were instrumental in the completion of this work.

I would also like to thank my instructors and colleagues at both the University of Oslo and the University of Saskatchewan. Your brilliance and opinions were truly inspirational. Thank you in particular to my close friend and classmate Oda Josephine Børke Selle; your light-hearted revisions and insight kept me sane throughout this journey.

Additionally, I would like to thank my family. To my parents – you taught me the meaning of perseverance and hard work. To my wife Jessica – your unending wisdom, patience, and understanding mean the world to me; I would not be where I am today without you.

Table of contents

1 Introduction

On December 31, 2019, the WHO received a report of an increase in cases of pneumonia caused by an unknown pathogen in Wuhan, China.[1] As of January 7, the cause was established as a novel coronavirus[2] (COVID-19), and in less than a week, on January 13, the first internationally imported case was reported by the Thai Ministry of Health.[3]

Countries scrambled to implement controls to prevent the introduction of cases; border closures started as soon as January 21, when North Korea banned all foreign tourists from entry.[4] Six countries[5] had implemented restrictions on international travel before the WHO declared a Public Health Emergency of International Concern (PHEIC) on January 30.[6] As the pandemic spread, states imposed measures in an attempt to control the introduction and spread of new cases, from closing borders to restricting international and domestic travel.[7] As of April 2020, every country in the world had imposed border restrictions of some nature to attempt to control spread by reducing or eliminating importation of cases through international border crossings.[8]

However, these controls did not prevent the importation of cases, only delaying them. As of the time of writing, only 11 countries in the world have not reported a positive case of COVID-19.[9] As a result, other methods of controlling disease spread were developed and implemented. Contact tracing has long been a method of monitoring and controlling communicable diseases,[10] and with recent technological advances, several nations in Europe and Asia implemented

---

[1] World Health Organisation, *Novel Coronavirus (2019 nCoV) Situation Report – 1* (Geneva: WHO, 2020) at 1.

[2] *Ibid*.

[3] *Ibid*.

[4] O'Carroll, C., & Weisensee, N., "Tourism to North Korea suspended amid China coronavirus concerns: operator", *NK News* (21 January 2020), online.

[5] Kiernan, S., & DeVita, M., "Travel Restrictions on China due to COVID-19", *Think Global Health*, (6 April 2020), online.

[6] World Health Organisation, *Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)* (Geneva: World Health Organisation, 2020), online.

[7] See generally Wells et al., "Impact of international travel and border control measures on the global spread of the novel 2019 coronavirus outbreak" (2020) 117:13 PNAS 7504.

[8] United Nations World Tourism Organisation, "100% of Global Destinations Now Have COVID-19 Travel Restrictions, UNWTO Reports", (28 April, 2020), online.

[9] Noroozi, E., "Which countries have not reported any coronavirus cases" *Al-Jazeera* (14 September 2020), online. Note that shortly after the publication of this article, Solomon Islands had a positive case, dropping the count from 12 to 11. See Radio New Zealand, "Solomon Islands has first case of COVID-19", *RNZ* (3 October 2020), online. Of these 11 counties, all but two are small pacific island states, and these two are states with oppressive, dictatorial regimes, being North Korea; see Aitken, P., "North Korea's Kim Jong Un again claims country has no coronavirus cases", *Fox News*, (10 October 2020), online) and Turkmenistan; see Abdurasulov, A., "Coronavirus: Why has Turkmenistan reported no cases?" *BBC News*, (7 April 2020), online.

[10] Contact tracing, long considered a key means of controlling the spread of communicable disease, has been used in some form since the 1920s. See Ohio State University, "Contact tracing's long, turbulent history holds lessons for COVID-19", (20 July 2020), online.

contact tracing applications – some are mandatory, others are optional.[11] Canada has recently developed and deployed its own contact tracing application, which it calls COVID Alert.[12]

This thesis will serve as an evaluation of COVID Alert, in the context of Canadian privacy law – considering how the application fits within the existing Canadian privacy law framework, and therefore whether what would otherwise be an intrusion on user privacy can be justified in the control of communicable diseases. The sub-issue that arises therefrom is an evaluation and commentary on the gaps and shortcomings of the existing Canadian privacy law framework, and how this may negatively affect the successful deployment of such a technology.

Comparative analysis will then be performed between the Canadian and European Union (EU) regimes to determine whether and how the Canadian framework could improve by adapting aspects of the law in force in Europe, and how this may affect contact tracing applications, as well as other technologies. Ultimately, this evaluation will conclude that the current state of the Canadian privacy regulatory framework is outdated and inadequate, suffering from unclear legislative drafting, inadequate enforcement provisions, and an outdated overall approach to privacy, as well as improper and inadequate jurisprudential interpretation of the *Privacy Act* by the Canadian courts. It will be concluded that updating statutory interpretation may solve some of these inadequacies, but wholesale revision of the Canadian privacy statutes is required to implement real change, though such efforts face significant hurdles in the form of federalism.

Such analysis is timely, considering there are forthcoming revisions to address theses shortcomings and inadequacies of the existing Canadian privacy legislation.[13] During the time this thesis was being drafted, the Canadian federal government has put forward proposed amendments, but it remains to be seen whether these proposed amendments will be adopted, whether in whole or in part, and whether this will functionally result in improvements.

1.1 Contact Tracing – Then and Now

Contact tracing is a process which has been utilized for decades to detect and track positive cases of communicable disease, with the ultimate goal to prevent the spread of disease.[14] When it comes to novel or emerging disease outbreaks, this requires the pathogen to first be identified,

---

[11] Most nations do not mandate these applications, instead using them as a part of a broader comprehensive program. However, there are nations which do require their use in certain applications. For example, in Thailand, the AOT Airport Application must be installed before any person passes through an airport immigration point, if a person has travelled to or is returning from a contagious area outside Thailand. See Norton Rose Fulbright, "Contact tracing apps: A new world for data privacy", *Data Protection Report*, (October 2020), online.

[12] Government of Canada, "Download COVID Alert Today" *Coronavirus Disease (COVID-19),* (30 October 2020), online. [GoC About COVID Alert]

[13] Government of Canada, "Modernizing Canada's *Privacy Act*", *Department of Justice*, (5 June 2020), online.

[14] Bland, S., "Reflections on the History of Contact Tracing", *O'Neill Institute for National & Global Health Law,* (13 July 2020), online.

then for the period of communicability[15] to be determined. The general premise of contact tracing then follows three steps: (1) identification of contacts, where a person who has tested positive for some communicable disease lists any activities they have done, or persons they have come in contact with; (2) listing of contacts, where names and contact information is gathered; then (3) follow-up, where those persons advised to monitor for symptoms and possibly referred for testing.[16] Note that determining who can be considered a contact often involves consideration of the pathogenicity of the particular communicable disease.[17]

As technology becomes more commonplace, approaches to contact tracing have shifted; several states have been working on developing and implementing contact tracing technologies and/or mobile applications – in 2010, the United Kingdom developed a means to digitally track influenza cases.[18] Mobile applications were tested for efficacy in tracking the spread of the Ebola outbreak in Sierra Leone from 2014 to 2016, and found that even in an environment with limited resources and connectivity, these applications are beneficial.[19]

Such applications do vary in their modes of operation, but are generally opt-in mobile applications, which track citizen movement to determine and notify when a user comes in contact with another user who is confirmed or presumed to be positive for communicable disease. Though an evaluation of the efficacy of contact tracing applications is outside of the scope of this paper, it is imperative to keep in front of mind that an intrusion on privacy for the claimed purpose of contact tracing cannot be justified if there is no discernible benefit.[20]

---

[15] The period of communicability (or period of infectiousness) is "the time interval during which an infectious agent may be transferred directly or indirectly from an infected person to another person"; see European Centre for Disease Prevention and Control, "ECDC Scientific Advice: Systematic review on the incubation and infectiousness/shedding period of communicable diseases in children", (June 2016) ECDC at iv.

[16] World Health Organisation, "Contact Tracing", *WHO Newsroom*, (9 May 2017), online.

[17] For someone to be a 'contact' of an HIV-positive person requires "contact between broken skin, wounds, or mucous membranes and HIV-infected blood or blood-contaminated body fluids" (see HIV.gov, "How is HIV transmitted?", *HIV Basics*, (24 June 2019), online), whereas contacts for airborne pathogens such as measles are those who enter a positive person's airspace within two hours of them coughing or sneezing (see Centers for Disease Control and Prevention, "Measles Transmission", *cdc.gov*, (5 November 2020), online).

[18] Owusu, P.N., "Digital technology applications for contact tracing: the new promise for COVID-19 and beyond?" (2020) 5:36, *Global Health Research and Policy* at 2.

[19] Danquah L.O., et al, "Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study" (2019) 19:810, *BMC Infectious Diseases* at 11.

[20] von Tigerstrom, B. *Information and Privacy Law in Canada*, (Toronto: Irwin Law, 2020) at 250. This conclusion is drawn from the concept of purpose limitation – that collection of personal information can only be justified where necessary for a specific purpose, in which case it can only be used and/or disclosed in accordance with that primary purpose, for other purposes which are directly related to the primary purpose, or where otherwise authorised by the law; other use or disclosure is *de facto* unlawful.

1.2 Current Examples of Application-Based Contact Tracing

The most common means of application-based contact tracing involves the use of an application-based interface combined with Bluetooth technology, which detects when two mobile devices are in close proximity. Upon two users coming within a pre-determined range, the application exchanges a unique code for each contact, so that if one user tests positive, the app pushes a notification to all other users who have logged that person's code as a contact.[21] Bluetooth-based applications are currently used by many different contact tracing applications worldwide, including those in Austria, Australia, Germany, Singapore, and Switzerland.[22] However, no technology is perfect, and critics of Bluetooth-based applications point to the fact that such applications require Bluetooth to be turned on, and left on, and that sensitivity depends on a user's individual location settings.[23]

There are several other approaches to contact tracing applications besides Bluetooth; there has been, and continues to be, significant debate over the most effective model, and how privacy concerns are to be balanced with COVID-19 control measures.[24] A thorough comparative analysis of these different technologies is beyond the scope of this thesis, but it is important to be aware that the efficacy of each technology varies, and therefore there is no "best" one-size-fits-all technology; each has advantages and drawbacks.

For example, applications which rely on the Global Positioning System[25] (GPS) are less precise than Bluetooth, and GPS accuracy is further diminished when a user is indoors, out of a direct line of sight of a satellite.[26] This is a significant drawback of GPS-based applications, as the majority of COVID-19 transmission has been found to occur indoors.[27] Supporters suggest GPS is preferable because most users do not regularly disable GPS when they are not using it, but this does not negate its precision issues.[28]

---

[21] Owusu, *supra* note 18 at 2.

[22] *Ibid*.

[23] Hernandez-Orallo, E., et al. "Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19" (2020) 8 *IEEE Access* 99083 at 99086; Government of Canada, "COVID Alert Privacy Notice (Exposure Notification)" *Public Health Services*, (13 November 2020), online [COVID Alert Privacy Notice]

[24] Pierucci, A., & Walter, J., "Joint Statement on Digital Contact Tracing (28 April 2020) *Council of Europe* at 3. See also at Council of Europe, "Digital Solutions to Fight COVID-19" (October 2020) *2020 Data Protection Report* at 18-19, 24-30.

[25] National Oceanic and Atmospheric Administration, "The Global Positioning System", *GPS.gov*, (22 April 2020), online. GPS is a method of location tracking utilising satellites in medium Earth orbit, which transmit and receive signals orbit around the earth in order to triangulate the location of the user.

[26] Hernandez-Orallo, *supra* note 23 at 99086.

[27] *Ibid*.

[28] *Ibid*.

Wi-Fi-based applications can be used to determine the identity of surrounding devices by documenting their Media Access Control (MAC) address,[29] negating the need for the generation of unique codes, and by utilising the received signal strength, can estimate another user's relative distance, which can be helpful in determining who is or is not a contact more precisely.[30] However, because these MAC addresses are unique to an individual piece of hardware, they are far more identifiable than unique codes generated by a device; therefore storing them on a remote server, as is done with unique codes generated by Bluetooth-based applications, raises greater concerns about privacy and data protection.

Finally, tracking by cellular networks is also possible. Seeing as cell providers already collect this information, there is an existing legal basis for collecting this data, and that data is presumably securely collected and stored. However, this user location data is less precise than that collected via other methods – in some areas, cellular tracking may only be accurate to within a hundred, or even a thousand metres, making the data effectively useless for contact tracing.[31]

1.2.1 The Canadian Application – COVID Alert

This paper will predominantly focus on the Canadian contact tracing application, called COVID Alert. COVID Alert does not use GPS, and it does not track the user's location.[32] Like many of the existing applications in other countries, it uses Bluetooth to exchange random codes with other phones nearby, which have their Bluetooth enabled and who also have the application.[33] The application checks the list of codes of persons who have reported via the application that they have tested positive for COVID-19, and then notifies the user if they have been near any of these persons in the past 14 days.[34]

On devices which have installed COVID Alert, the Google/Apple Operating System (GAOS) layer generates a temporary exposure key, which in turn generates a rolling proximity identifiers (RPI) approximately every 5-25 minutes.[35] RPIs are shared with other devices using COVID Alert, and which are used to generate a temporary exposure key (TEK) which is stored on the device, until a user tests positive for COVID-19, at which point it is uploaded to the server.[36]

---

[29] Office of Information Technology, "Find Your MAC Address", *UCInet* (20 October 2020), online. MAC addresses are hardware-level addresses of the physical card or chip in your device which allows access to the internet. As such, it can be traced back to an individual device with relative ease.

[30] Hernandez-Orallo, *supra* note 23 at 99086.

[31] *Ibid*.

[32] GoC About COVID Alert, *supra* note 12.

[33] *Ibid*.

[34] *Ibid*.

[35] Government of Canada, *COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment*, October 2020, online. [COVID Alert Assessment]

[36] *Ibid*.

The application does not track, nor does it know, user names, address, locations, contacts, or health information.[37] At this time, the only means of the application becoming aware a user has tested positive for COVID-19 is by that user self-reporting their diagnosis, which is optional, and requires user consent. At the time of writing, users may only self-report if they are in one of seven provinces – Manitoba, New Brunswick, Newfoundland, Ontario, Prince Edward Island, Quebec or Saskatchewan.[38] Self-reporting is done using a key that is given to the user by a healthcare provider from their Provincial or Territorial Health Authority (PTHA); the user does not directly input their diagnosis in to the application.

It is also important to be aware that, as a security measure, the user's IP address is logged when the application downloads a list of positive codes, enters a one-time key as a result of a positive diagnosis, and/or when the user uploads their random codes.[39] However, the user's IP address is not connected to any other information generated, collected, or used by the application, and is logged to prevent and investigate cybersecurity concerns.

In-depth analysis of the operation of COVID Alert, as well as analysis of whether, and to what extent, operation of the application is in compliance with applicable and relevant federal law, will be covered in greater detail in section 2.2 of this thesis.

2 Canadian Regulatory Framework

To state that the Canadian privacy law framework is complex is an understatement. There are two federal acts purporting to regulate privacy in Canada; the first is the *Privacy Act*, which applies to processing of personal information by crown corporations and federal government institutions listed in Schedule 3.[40] The second is the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to the private sector, when they collect, use, or disclose personal information in the course of a commercial activity.[41] There are also a number of regulations under each of these acts, none of which are directly relevant for this paper.

---

[37] GoC About COVID Alert, *supra* note 32.

[38] *Ibid*.

[39] This is important to note primarily because there is literature which suggests IP addresses are, in fact identifiable information, including reports from both the Government of Canada and the Privacy Commissioner of Canada, which state IP addresses can be connected to an individual by using information available from other sources, such as internet service providers, or via improvements in available technology. This will be discussed in further detail later in this paper, under 4.1.1. See Government of Canada, "Privacy" *Canada.ca*, (2 November 2020), online [GoC Privacy Policy]; Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You", *Technology Analysis Branch,* (May 2013) at p 7. [OPCC IP Addresses]

[40] *Privacy Act*, RSC 1985, c P-21 at s 2 stipulates "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.". Schedule 3 outlines what is included in the term "government institution".

[41] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 at s 4. [PIPEDA]

In addition to the two federal acts, every Canadian province has enacted some form of provincial privacy law; there are a total of 31 provincial statutes, with regulatory capacity and applicability varying by province.[42] Every province has enacted some form of provincial public sector privacy law, and some have also enacted provincial statutes to either supplement, or either partly or fully replace, PIPEDA. For example, Alberta, British Columbia, and Quebec all have enacted their own provincial private sector privacy statutes, which have been deemed "substantially similar" to PIPEDA; therefore these provinces are exempt from PIPEDA "with respect to the collection, use or disclosure of personal information that occurs within that province".[43] Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador are considered to have "substantially similar" legislation to PIPEDA, but only for the collection, use and disclosure of personal health information.[44] For the purposes of this paper, given the Canadian contact tracing application was developed and implemented at the federal level, these provincial statutes will largely be considered out of scope.

2.1 Canadian Federal Privacy Law

Canadians do not have an explicit right to privacy *per se*; neither the Canadian Constitution[45], nor the Canadian Charter of Rights and Freedoms[46] directly mention either privacy or data protection. Depending on the circumstances, privacy may be considered to be indirectly protected under either section 7 or 8 of the Canadian Charter of Rights and Freedoms.[47]

Canadian privacy law deals with what the statutes define as "personal information". As introduced above, Canada has two federal acts relating to privacy, and they can be differentiated by scope. PIPEDA pertains to data collected, processed and/or stored by the private sector, whereas the *Privacy Act* regulates data collected, processed and/or stored by the public sector.

2.1.1 Privacy Law in the Private Sector – PIPEDA

PIPEDA is a relatively new statute, having come into effect less than 20 years ago in response to the increasing popularity of e-commerce, and to ensure Canadian adequacy for data transferal under the European Union's Data Protection Directive.[48] The purpose of PIPEDA is as follows:

---

[42] Office of the Privacy Commissioner of Canada, "Provincial and territorial privacy laws and oversight", *About the OPC*, (11 June 2020), online.

[43] Office of the Privacy Commissioner of Canada, "PIPEDA in Brief", *The Personal Information Protection and Electronic Documents Act*, (7 June 2020), online. [PIPEDA in Brief]

[44] *Ibid*.

[45] *Constitution Act*, 1867, 30 & 31 Victoria, c 3 (UK).

[46] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

[47] von Tigerstom, *supra* note 20 at 12. Section 7 of the *Canadian Charter of Rights and Freedoms*, *supra* note 26 preserves the right to life, liberty, and security of the person; section 8 is the right to be secure against unreasonable search and seizure.

[48] von Tigerstom, *supra* note 20 at 292.

> "*to establish… rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.*"[49]

PIPEDA applies, in accordance with section 4(1), when personal information[50] is collected, used or disclosed for a federal work, undertaking, or business, or for a commercial activity. However, if a province has substantially similar legislation, it is possible for an actor which would otherwise by bound by PIPEDA to be exempted from application, but only insofar as that activity takes place entirely within the bounds of that province.[51]

The complex applicability of PIPEDA contributes to its weak status, as does its awkward drafting.[52] The process of updating and modernising Canadian privacy law, including PIPEDA, is ongoing, but whether and to what extent the revisions will improve the statute remains to be seen. Considering that COVID Alert was developed and implemented by the public sector, it is more important to evaluate the *Privacy Act*, but this does not mean PIPEDA is irrelevant. The lines between the public and private sectors are blurring,[53] leading to questions of whether this statutory divide between public and private sectors remains an appropriate legislative approach.

2.1.2 Privacy law in the Public Sector – the *Privacy Act*

In contrast to PIPEDA, the *Privacy Act* applies to the collection, processing, and storage of personal information[54] by public bodies and government institutions.[55] Interpretation of this statute is complicated by the fact the Federal Court of Appeal held the *Privacy Act* and PIPEDA cannot be interpreted in the same way, as their purposes are "altogether different".[56]

---

[49] PIPEDA, *supra* note 41 at s 3.

[50] *Ibid* at s. 2(1) defines personal information as "information about an identifiable individual"

[51] PIPEDA in Brief, *supra* note 43.

[52] See generally von Tigerstrom, *supra* note 20 at p. 294-5. When PIPEDA was drafted, it integrated a Canadian Standards Association Model Code, rather than adapting it. A CSA Code is drafted entirely differently than a statute, resulting in ambiguous language, compromised form, and provisions open to interpretative arguments.

[53] This will be further discussed under section 4.2; COVID Alert was developed in conjunction with Apple and Google, as an application operating on their platforms, and which must interface with their respective operating systems. COVID Alert Assessment, *supra* note 35, does not mention this tension; presumably, the operating system layer does not have access to any part of the operation of the application (though this is unconfirmed; a deep dive in to application source code is beyond the scope of this paper).

[54] *Privacy Act*, *supra* note 40 at s 3 defines personal information as "information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing..." and goes on to list several different categories, including, notably, "**(c)** any **identifying number, symbol or other particular** assigned to the individual" (emphasis added). In contrast to PIPEDA, this definition is more thorough.

[55] Note the statute has authority to exclude public bodies from applicability – notably, political parties and courts are generally excluded from the application of the *Privacy Act*; see von Tigerstrom, *supra* note 20 at 234.

[56] *Englander v Telus Communications Inc*, 2004 FCA 387, at para 38.

The purpose of the *Privacy Act* is "to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."[57] Further, "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."[58]

Determining whether the *Privacy Act* applies requires consideration of three criteria. Firstly, a Government Institution must be involved.[59] If a Government Institution is involved, there must be (1) collection of (2) identifiable personal information. Collection involves gathering or receiving of personal information not already in the possession of the public body, and does include obtaining personal information from any source, even those that are publicly available.[60] As a matter of default, personal information ought to be collected directly from the data subject,[61] and that person must be informed as to the purpose of the collection, the authority which allows collection, and contact information which the subject may use to ask questions.[62]

Collection is subject to limits, and requires a legitimate purpose.[63] Under the federal *Privacy Act*, personal information can be collected only if "it relates directly to an operating program or activity of the institution".[64] Note the wording – "relates directly" is not "necessary"; this has been confirmed by the Federal Court of Appeal, which held that Parliament would have written "necessary", had that been their intention.[65] Accordingly, the test of determining whether collection "relates directly" becomes a "less onerous test of establishing a direct, immediate relationship with no intermediary between the information collected and the operating programs or activities of the government".[66] Whether or not COVID Alert meets this test, as well as whether this is an appropriate standard, will be analysed in further detail in the following sections.

To this end, the following sections will also address the roles of data matching and/or linkage; it is therefore important to highlight what this process entails, and where it is permitted. Data

---

[57] *Privacy Act*, *supra* note 40 at s 2.

[58] *Ibid* at s 4.

[59] *Ibid* at Schedule 3.

[60] von Tigerstrom, *supra* note 20 at 250-251

[61] *Ibid* at 252.

[62] *Ibid*.

[63] *Ibid* at 253.

[64] *Privacy Act*, *supra* note 40 at s 4, as cited by von Tigerstrom, *supra* note 20 at 254.

[65] *Union of Correctionnel* [*sic*] *Officers* v *Canada (Attorney General)*, 2019 FCA 212 at para 40; Boivin, JA, goes on to state in para 41 that this ambiguity has always been present, and the Privacy Commissioner has twice attempted to have Parliament reform this provision to include a "necessity test". Curiously, Boivin, JA, goes on to indicate at para 43 that "most, if not all, of the provincial equivalents of this provision contain explicit references to the notion of necessity".

[66] *Union of Canadian Correctional Officers - Syndicat des Agents Correctionnels du Canada - CSN (UCCO-SACC-CSN)* v *Canada (Attorney General)* 2016 FC 1289 at para 141.

matching/linking is a form of information sharing, whereby personal information in one server or database is connected with personal information obtained from elsewhere. This process can increase identifiability, and is considered to constitute indirect collection of personal information.[67] This becomes an issue because the general rule is such that all information ought to be collected directly from individuals who have been informed of the purpose(s) of said collection. [68] Though indirect collection is permitted in certain circumstances, the party matching the information must have legal authority.[69] The circumstances in which data matching may be performed in the context of COVID Alert will be discussed in further detail below.

The element of identifiability is also highly relevant to this analysis, being contained in both the explicit and implicit definition of personal information.[70] The threshold for determining identifiability of personal information has been held to be where the information poses a "serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information".[71] This holding has since been followed in subsequent judgements in the Canadian Federal Court.[72] The extent to which this standard applies to information collected by COVID Alert insofar as that information is identifiable will be analysed further in the following sections. Usage of personal information is also limited to the purposes for which it was originally collected (the primary purpose),[73] for other uses consistent with the primary purpose,[74] for other purposes where consent is obtained,[75] or for disclosure[76] (where that disclosure is limited to public bodies, in pursuit of the primary or subsequently consistent purposes, with consent, or in accordance with statutory provisions).[77]

Though data security is not the focus of this paper, it is also important to address that the implementation of adequate safeguards is imperative to any application handling information

---

[67] von Tigerstrom, *supra* note 20 at 277.

[68] *Ibid* at 277-278.

[69] *Ibid.*

[70] *Privacy Act*, *supra* note 40 at s 3.

[71] *Gordon* v *Canada (Minister of Health)*, 2008 FC 258, at para 34 [*Gordon*]

[72] *Canada (Information Commissioner)* v *Canada (Minister of Public Safety and Emergency Preparedness)* 2019 FC 1279 at paras 34-35 [*Canada Info Comm*].

[73] *Privacy Act*, *supra* note 40 at s 7(a).

[74] *Ibid*.

[75] *Ibid* at s 8(1); for example, disclosure.

[76] *Ibid* at s 7(b).

[77] von Tigerstrom, *supra* note 20 at 259-60. Use is further limited in several ways beyond this definition; usage and disclosure should be limited to circumstances where it is "reasonably necessary", and disclosure or use of more personal information than is "reasonably necessary" may violate the statute. Furthermore, the Federal Court has held that where disclosure is permitted, public bodies "should consider alternatives to full disclosure in order to strike a balance between the need for disclosure and the right to privacy." See *Canada (Minister of Public Safety and Emergency Preparedness) v Kahlon*, 2005 FC 1000 at para 37, and *Canada (Minister of Public Safety and Emergency Preparedness) v Lin*, 2011 FC 431 at para 36, which cites *Kahlon*.

which may be potentially considered personally identifiable. Such safeguards can relate to principles of data minimisation,[78] the need-to-know principle,[79] and ensuring data integrity.[80] This is especially important when the information in question may involve relatively sensitive topics, such as whether someone has contracted a communicable disease.

2.1.3 Federalism and Canadian Privacy Law

This framework can easily be construed as fragmented, disjointed, and nonsensical by persons unfamiliar with the tenets of Canadian constitutional law. A major contributing factor for the existence of this unconventional framework is federalism.

Sections 91 and 92 of *The Constitution Act*,[81] provide for the division of powers under the Canadian Constitution, dictating what areas fall under the purview of the federal and provincial governments respectively. However, as not every possible jurisdictional area was contemplated when the statute was drafted, conflicts arise when a new area or industry develops which requires regulation, which did not exist or was not considered in 1867.[82] Such is the case of privacy and data protection – this area is not explicitly assigned to either the federal or provincial governments under ss. 91 or 92, and therefore neither level of government has the explicit authority to regulate it.[83]

As a result, privacy and data protection is regulated as subsets of enumerated federal or provincial powers. The federal government has the authority to regulate trade and commerce,[84] ergo the federal government can implement PIPEDA, regulating personal information in the private sector. Provincial governments have the authority to regulate healthcare,[85] as well as purely

---

[78] von Tigerstrom, *supra* note 20 at 282 defines data minimisation as "using and disclosing the minimum amount of personal information necessary for the purpose"

[79] *Ibid.* The need-to-know principle is defined as "ensuring that persons within an organization have access to only the personal information needed to perform their functions"

[80] *Ibid*. Ensuring data integrity is defined as ensuring data are "protected against loss, damage, or alteration"

[81] *Supra* note 45.

[82] This is a relatively common problem, especially in technological advancements. The commercialisation of airplanes and airports and the resulting need for regulation was another area which the federal and provincial governments fought for the jurisdictional right to regulate. See generally *Reference re legislative powers as to regulation and control of aeronautics in Canada*, [1930] S.C.R. 663. Most recently, the constitutionality of a federal carbon tax has been challenged, partly for similar jurisdictional disagreements, by the Alberta, Ontario, and Saskatchewan provincial governments as an infringement of provincial sovereignty; the Supreme Court of Canada has not yet handed down their decision on this issue. See Ma, C., & da Silva, E., "Supreme Court of Canada hears carbon tax constitutionality appeals, *Miller Thompson News*, (25 September 2020), online.

[83] See von Tigerstrom, *supra* note 20 at 6.

[84] *Constitution Act*, *supra* note 45 at 91(2).

[85] Jackman, M, "Constitutional Jurisdiction Over Health in Canada" (2000) 8 Health Law Journal 95 at 96. The *Constitution Act*, *supra* note 45 at 92(7) gives jurisdiction over hospitals; when combined with powers under 92(13) (property and civil rights), and 92(16), (matters of a merely local or private nature), this has been extended to cover provision of healthcare in general.

local and private matters,[86] hence provincial governments being permitted to implement their own private sector regulations for business conducted entirely within that province, as well as privacy acts regulating health information.

The result is a complex, internally conflicting regulatory framework. Neither federal nor any provincial governments readily relinquish regulatory authority to the other; provinces actively fight the federal government for jurisdiction over several areas, including the right to legislate privacy.[87] Unfortunately, because of this hesitancy to relinquish control, and the complex, delicate process required for constitutional reform (which would be necessary to rewrite section 91 or 92 to include privacy and data protection as either a provincial or federal power)[88] it is extremely likely that Canada is, for the foreseeable future, stuck with these federalism issues.

It is therefore exceedingly unlikely, if not outright impossible, for Canada to adopt the EU's approach and unilaterally impose a broad, all-encompassing statute such as the General Data Protection Regulation (GDPR)[89] which purports to regulate every aspect of privacy law. However, this isn't to say that the Canadian privacy law framework could not still learn from or adapt elements of the GDPR or its interpretation, in order to modernise and improve the existing privacy law regime. Such possibilities will be investigated under section 4 of this thesis.

2.2 Applying the *Privacy Act* to COVID Alert

In this section, two aspects will be evaluated – firstly, what information is being collected by COVID Alert, and relatedly whether that process constitutes "collection" under *The Privacy Act*. If information is being collected, then secondly, it must be determined whether that information can be considered "identifiable".

As a preliminary point, the question of *who* is "collecting" the information in question must be answered; if the entity doing the collecting is not a Government Institution under the *Privacy Act*, then even if that information is identifiable, the *Privacy Act* would not apply.[90] COVID Alert was developed by an interdisciplinary team, which included Health Canada, Canadian

---

[86] *Constitution Act*, *supra* note 45 at 92(16).

[87] See von Tigerstrom *supra* note 20 at 293, where provincial constitutional challenges of PIPEDA are discussed.

[88] See generally Albert, R. "The Difficulty of Constitutional Amendment in Canada" (2015) 53:1 AB Law Reform 85 at 86 which concludes that though the United States Constitution is on widely considered one of the most difficult to reform in the world, it may well be that Canada's would be harder. Attempts to reform the Canadian Constitution could either (a) be supplanted by a province to subvert the process of constitutional reform to further their own political agenda (at 100) , and/or (b) would likely face extreme pushback from whichever level of government the authority was being taken from.

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

[90] As per the *Privacy Act*, *supra* note 40 at s. 2.

Digital Service (CDS), ISED (Industry, Science and Economic Development) and the Canadian Centre for Cyber Security (CCCS).[91] Of these four organisations, Health Canada is the lead – charged with overall implementation of the application, assessing privacy risks and implications, engaging with the Office of the Privacy Commissioner, and driving uptake.[92] Health Canada falls under the Health Portfolio, and therefore is subject to the *Privacy Act*, which enshrines the Department of Health as a Government Institution.[93] CDS, as mentioned, predominantly provides internal IT support to Health Canada, but also physically developed the application, operates the key server, stores diagnosis keys, and provides provincial and territorial health authorities (PTHAs) with access.[94] CDS also owns and is responsible for the operation of the servers which collect and store IP addresses, via the previously described process, though these servers are separate and distinct from those which receive, store, and transmit TEK codes.[95] CDS is supported by the Office of the Chief Information Officer, which is a branch of the Treasury Board of Canada Secretariat Organisation,[96] an enumerated Government Institution.[97] ISED and the CCCS are not involved with the ongoing operation of the application *per se*, ISED continues to be involved in supporting the governance and the roll-out of the application, and CCCS provides cybersecurity advice and guidance on systems design.[98]

In summary, key members of the multidisciplinary team responsible for development and operation of COVID Alert are Government Institutions under jurisdiction of the *Privacy Act*.[99] In the published Privacy Assessment of COVID Alert, reference is made to the "Government of Canada" – presumably, this is in reference to this interdisciplinary team, or members thereof. Accordingly, when referring to this Privacy Assessment, any reference to the "Government of Canada" hereafter entails a Government Institution under the purview of the *Privacy Act*.[100]

2.2.1 Is COVID Alert Collecting Information?

In considering this question, it is important to note the "Government of Canada" performed a privacy assessment of COVID Alert, considering both (a) whether there is "collection" of personal information, and (b) whether that information is identifiable.[101] The assessment concluded

[91] COVID Alert Assessment, *supra* note 35.

[92] *Ibid*.

[93] *Privacy Act*, *supra* note 40 at Schedule 3.

[94] COVID Alert Assessment, *supra* note 35.

[95] COVID Alert Privacy Notice (Exposure Notification), *supra* note 23.

[96] Government of Canada, "Treasury Board of Canada Secretariat Organisation", *Canada.ca*, (27 July 2020), online.

[97] *Privacy Act*, *supra* note 40 at Schedule 3.

[98] COVID Alert Assessment, *supra* note 35.

[99] *Privacy Act*, *supra* note 40 at Schedule 3.

[100] *Ibid*.

[101] COVID Alert Assessment, *supra* note 35.

collection is performed, a conclusion with which I do not disagree.[102] However, this assessment also claims the information is not identifiable, a claim which I will dispute in section 2.2.2.

Collected data elements include RPIs, TEKs, diagnosis keys, province of residence,[103] one-time keys from PTHAs, and the associated metadata for each of these elements.[104] Each of these elements, specifically to what extent they are being "collected" will be considered in further detail in the remainder of this section; the following outlines and conclusions are taken from the information provided by the "Government of Canada's" COVID Alert Privacy Assessment.[105] Much of the following analysis is high-level, since, as indicated, collection is less the issue than whether or not these data are identifiable.

As introduced in section 1.2.1, RPIs and TEKs are generated by the application on the GAOS[106] layer.[107] RPIs are generated approximately every 5-20 minutes and are affiliated with the TEK. RPIs are what is transmitted via Bluetooth to and from other devices; the GAOS layer logs and stores the RPIs of other devices which the user comes in proximity with. A TEK is generated once per day, and as a general rule, are stored locally on the device which generates and/or collects them for 14 days, at which time they are deleted. TEKs are only uploaded to the server with user consent, and only when the user self-reports a positive diagnosis for COVID-19.

When a user tests positive for COVID-19, PTHAs who have adopted COVID Alert provide that user with a one-time code which is inputted into the application. The application validates the code and asks for consent to upload the user's past 14 days' worth of TEKs to the Government of Canada server.[108] If the user grants consent, there is communication with the GAOS layer, consent is confirmed, and the TEKs are uploaded to the key server (at which point these non-expired TEKs technically become diagnosis keys). Other user's applications download these uploaded keys every day, the GAOS layer regenerates the RPIs from each of the downloaded

---

[102] *Ibid*. Data elements are collected during the operation of COVID Alert, for the purposes of contact tracing, by Health Canada and CDS, which are Government Institutions under *Privacy Act*, *supra* note 40, Schedule 3.

[103] Note this is optional – a user is not required to select their province of residence for the application to operate.

[104] COVID Alert Assessment, *supra* note 35. The key example of associated metadata which will be considered in this analysis are IP addresses, which will be discussed in greater detail in later sections.

[105] *Ibid*.

[106] *Ibid*. Recall GAOS stands for Google/Apple Operating System, the operating system for the particular handheld mobile device generates the TEK; Google for Android devices, and Apple for iPhone and other iOS devices.

[107] *Ibid*, "The design of the Google/Apple API is such that this protected layer of the operating system is isolated, so no other app on the device can access its data, and even the exposure notification app can only access the data through explicit user consent. Only one app per device can access the Google/Apple layer, and only one app per geographical region is permitted."

[108] Note here that consent is sought for disclosure of this information, see *Privacy Act*, *supra* note 40, at s 8.

diagnosis keys, and if those keys match any of the keys on the user's device, and exposure criteria are met[109] the user is notified they have been exposed to COVID-19.

Users may be asked additional information at the time of application set up and upon entering a key from their PTHA. For example, at the time of installation, users may be asked their province or territory of residence. Provision of this information is not mandatory and does not seem to impact the functionality of the application. It is unclear what purpose the collection of this data may provide, outside of presumably tracking uptake by province or territory.

Upon entering the one-time key, the user will also be asked the date they first started to experience symptoms that prompted them to get tested; if the user cannot remember or is asymptomatic, the user will be advised to input the date they received their test. Answering these questions is optional and is only used to determine the dates that the user may have been infectious[110] so that only the TEKs of the dates for which they were infectious are uploaded. If the user does not provide this information, the TEKs from the 14 days preceding the self-reported positive diagnosis will be reported. This is seemingly done in accordance with the principle of data minimisation; only relevant data, to which the user has also granted consent, is disclosed.

It is important to note that metadata, the most relevant of which is IP addresses, are collected and stored any time a request is made involving the server; for example, when a user uploads their TEKs, or enters a PTHA code. IP addresses are collected and stored in one of two locations. If an invalid PTHA key is entered, the IP address of the user attempting to utilise that key will be logged for a rolling 60-minute period on the Government of Canada key server used for the COVID Alert application, after which point the IP address is deleted. After 50 consecutive incorrect attempts from the same IP address, that IP will be blocked for 60 minutes. Though not directly stated as such by the Government of Canada, this process is presumably in place to prevent distributed denial of service (DDoS) attacks.[111]

IP address are also stored in access logs, on a separate server for 3 months, unless the log is implicated in a security investigation, in which case, the log may be stored for up to 24 months. The reasoning for this collection is cited as being intended "to adequately understand, monitor, and respond to attacks against a system and for the secure and reliable operation of the service".[112] The Government of Canada claims IP addresses would not be used by CDS to identify

---

[109] This is a continuous 15-minute exposure period. See COVID Alert Assessment, *supra* note 35.

[110] *Ibid*. If this information is provided, the Government of Canada claims this period is considered to be two days before onset of symptoms or the date the test was performed.

[111] This is a type of attack whereby malicious actors flood a website or service with more traffic than that service is capable of handling, causing it to crash. See Weisman, S., "What is a distributed denial of service attack (DDoS) and what can you do about them?" *Norton Emerging Threats*, (23 July 2020), online.

[112] COVID Alert Assessment, *supra* note 35.

persons or the source of attacks, claiming it lacks the resources to do so, but would disclose to the law enforcement in the event access to the database was attempted or successfully achieved.

2.2.2 Is the Data Collected by COVID Alert Identifiable?

Having established data is collected for the purpose of the operation of the application, it must be considered whether the data is identifiable personal information. The *Privacy Act* does not define "identifiability"; however, this lack of a clear statutory definition is not necessarily negative *per se*; it is, to some extent, inevitable that courts will need to interpret a statute.

When looking to the courts for assistance in determining what is "identifiable", it is revealed that different courts have generated different definitions. The Supreme Court of Canada has held that the interpretation of "identifiable" is intended to be broad,[113] insofar as the definition captures a wide array of potential data. However, the Supreme Court has not provided an actual definition of "identifiable", so this has fallen to the lower courts, several of which have held different interpretations. The Federal Court of Canada has held that the test is whether there is a "serious possibility" of an individual subject being identified via the information in question, whether "alone or in combination with other information."[114] On the other hand, the Ontario Court of Appeal, a provincial-level appellate court, has held that the standard is whether there is a "reasonable expectation" that the data subject could be identified.[115] Whether and to what extent these interpretations are either similar or dissimilar is not entirely clear.

As a further point of consideration, setting aside the fact that province of residence is asked when the application is first initialised,[116] personal information, according to von Tigerstrom, "must also be 'about' the individual in the sense that it reveals something personal".[117] A holistic consideration of this "about" factor, especially in consideration of this section's analysis of identifiability, likely leads to a conclusion that persons who come in close contact with the user are certainly data "about" the user. It could point to close social contacts, sexual partners, family relations, or any other possible factors, all of which are certainly data "about" a person.

As introduced in the preceding section, the "Government of Canada" performed a privacy assessment of COVID Alert, which considered whether information collected by COVID Alert

---

[113] *Dagg v Canada (Minister of Finance)* [1997] 2 SCR 403, at paras 68-69; though this broad interpretation of "identifiable" was held by LaForest J in dissent, the majority concurred on this point.

[114] *Gordon*, *supra* note 71; *Canada Info Comm*, *supra* note 72.

[115] *Ontario (Attorney General) v Pascoe*, [2002] O.J. No. 4300 (CA) at para 2.

[116] As mentioned above, this information is optional. A person's address is considered identifiable, as per *Privacy Act*, *supra* note 40 at s. 3, but the province of residence alone is not an address per se. That said, this is important to note because it is possible that this can be utilised as linking information to render other information identifiable, as will be discussed later in this section.

[117] Von Tigerstrom, *supra* note 20 at 238, citing *Canada (Information Commissioner)* v *Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157.

is identifiable.[118] It concluded the risk of the data in question being identifiable is so low so as to fail to meet the "serious possibility"[119] threshold of identification;[120] stating *inter alia*:

> "it is so highly unlikely that an individual could be identified, that the collection of data elements (including IP addresses) and how they are used does not meet the threshold of "serious possibility" that an individual could be identified."[121]

I do not agree with this conclusion. I propose that there are three distinct potential circumstances where there are compelling arguments to be made for the conclusion that some or all of the information collected by COVID Alert may be identifiable. These three categories are (1) data which are identifiable by the government institutions at the time the data are collected, (2) information which is identifiable as a result of disclosure to third parties, and (3) information which can be made identifiable by malicious third parties. I will now consider each of these three categories in greater detail.

2.2.2.1 Data identifiable by the government institution(s) at the time of collection

The Government of Canada seems to consider that information collected by COVID Alert is not identifiable, and from their exclusive perspective, they may be partly correct. Most of the information collected by Government Institutions for the operation of COVID Alert, examined in the absence of any other information, is probably not identifiable. In order to render RPIs, TEKs, and exposure keys identifiable would require additional information be linked to, or combined with, the collected information. The reality is that these Government Institutions would appear to (a) have no reason to undergo this linking or combination process, and (b) not have ready access to the required linking information; therefore, viewed exclusively from their perspective, much of the collected data is probably not identifiable.

That said, IP addresses remain a major point of contention under this category. As mentioned above, IP addresses accompany the TEK codes sent to the server when a user self-reports their positive diagnosis; they are metadata, part of that data traffic, and are required for base functionality. As a base function of the operation of the internet, IP addresses accompany any request made to or from a website or online server.[122]

The Government of Canada claims that IP addresses, at least insofar as they are collected for the operation of COVID Alert, are not identifiable, and that any access to them is highly

---

[118] COVID Alert Assessment, *supra* note 35.

[119] *Gordon*, *supra* note 71; *Canada Info Comm*, *supra* note 72.

[120] COVID Alert Assessment, *supra* note 35. Notwithstanding, the Government of Canada claims to have safeguards in place to protect collected data, that security is partly guaranteed through minimised retention times, and that the application nonetheless adheres to all requirements of the *Privacy Act*, *supra* note 40.

[121] COVID Alert Assessment, *supra* note 35, citing *Gordon*, *supra* note 71.

[122] OPCC IP Addresses, *supra* note 39 at Annex A.

restricted.[123] The Government of Canada claims CDS lacks the technical capacity to connect an IP address to an individual smartphone and/or individual, but does not state why they believe that to be the case, merely claiming it would require "sophisticated analysis (beyond CDS's capabilities), or access to the subscriber lists of Internet service providers".[124] The government further claims "this is a non-public disclosure with a low possibility of attack and a low impact, meaning the risk tolerance should be higher."[125]

However, this seems to be inconsistent with two issues. Firstly, it is arguable that the data in question (being the status of a person's diagnosis with a communicable disease) constitutes, or relates to, health information, which ought to be held to a higher standard of protection.[126] Secondly, it is inconsistent with what is currently considered the norm, that technology has expanded the purview of what is identifiable. Given the amount of information available online, it can take only a very small amount of digital information, obtainable via a Google search, to render information which was once thought to be anonymous, identifiable.[127] IP addresses, in particular, even non-static IPs, can be fairly easily be pinpointed to an individual.[128]

This conclusion that IP addresses are not identifiable is also in conflict with existing Canadian jurisprudence,[129] as well as the Government of Canada itself – which has concluded in an assessment of its own website that IP addresses are personal information, insofar as the Government of Canada can, by their own admission, legally obtain sufficient and adequate information from internet service providers to identify an individual by their IP address.[130] A mere promise by the federal government that they will not link this data does not preclude them from the *possibility* that it *could* be done. Furthermore, as technology continues to improve, and individuals continue to register their own domains, this linking information is no longer only available through a formal request to an internet service provider; it may be publicly available.[131]

---

[123] COVID Alert Assessment, *supra* note 35, citing *Gordon*, *supra* note 71.

[124] COVID Alert Assessment, *supra* note 35.

[125] *Ibid*.

[126] Such is the case under the GDPR, which prohibits processing of "special categories of personal data", which includes health data, without meeting one or more specified exceptions. See GDPR, *supra* note 89 at Art. 9. However, it is also important to note that the reason the *Privacy Act* does not speak to health information is due to the federalism issues this would raise, as introduced under section 2.1.3 of this paper; jurisdiction over health resides with the provincial, not federal government. See the *Constitution Act*, *supra* note 45 at s. 92.

[127] OPCC IP Addresses, *supra* note 39.

[128] *Ibid.* International courts have also been willing to acknowledge this point; see C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, in which it was held that dynamic IP addresses ***are*** personal data where the IP address itself is recorded by the website operator, who is lawfully able to gain access to information stored by ISP that can identify user behind the address.

[129] See, for example, *R v Spencer*, 2014 SCC 43 at para 25.

[130] GoC Privacy Policy, *supra* note 39

[131] OPCC IP Addresses, *supra* note 39 at endnote 4-5, 7.

For these reasons, I disagree with the Government of Canada's claim that the possibility an individual could be identified is so extraordinarily low that it fails to meet the threshold of a "serious possibility" of identification. Such a stance is inconsistent with current technologies, literature, jurisprudence, and the Government of Canada's own claims. These inconsistencies have not been clarified by the Government of Canada in respect to COVID Alert, perhaps suggesting the need for jurisprudential clarification of the definition of identifiability, or if not, that perhaps that Parliament ought to look towards codifying identifiability.

2.2.2.2 Data which are identifiable purely as a result of disclosure

There are also issues whereby personal information collected by the application may become identifiable through the process of disclosure. Consider, for example, the disclosure of a diagnosis key; whereby a user's application has downloaded TEKs for other users who have tested positive, the application detects an RPI match, and notifies the user that they have been exposed.

Concerns around identifiability in this case arise when considering the nature of the parameters which the Government of Canada has decided upon to meet the criteria of an "exposure". The COVID Alert application only considers users to have been "exposed" to one another when they have been in continuous contact for more than 15 minutes.[132] However, persons are consistently advised by federal and provincial governments to keep social circles small, avoid public gatherings, and minimize trips away from the household or work environments.[133] Accordingly, it is fair to assume that as a result of these policies, the list of possible persons the exposure could be attributed to will shrink significantly, potentially to as small as one or two persons.

Therefore, when COVID Alert notifies a user that they have been exposed, they are effectively disclosing that someone they have been in close proximity to for more than 15 minutes in the last 14 days or less, who is also a user of COVID Alert, has tested positive for COVID-19. Again, consider that the list of persons who fit these criteria could be as short as 1-2 persons, especially if the user has been diligent about shrinking their social circle. Personally, reflecting on my exposures in the last 14 days, there are only two persons who meet this definition outside of my home, and both are in the same household.

It is therefore entirely reasonable to argue that this notification effectively amounts to disclosure. The information by nature of being disclosed is not necessarily any more or less identifiable *per se*, nor will the disclosure be *de facto* unlawful in this particular context,[134] but the

---

[132] COVID Alert Assessment, *supra* note 35.

[133] Government of Canada, "Coronavirus disease (COVID-19): Prevention and risks", *Canada.ca*, (3 November 2020), online.

[134] As per the *Privacy Act*, *supra* note 40 at s 8. As has been explained, the user, when they upload their diagnosis key, is asked for consent before this information is uploaded to the server and made available to other application users. See COVID Alert Assessment, *supra* note 35.

context of the disclosure may be capable of rendering the information identifiable, contrary to the claims made by the Government of Canada. The issue here is that the Government of Canada is misrepresenting the anonymity of TEKs and diagnosis keys in these circumstances, by assuring the user that their identity will be protected, when there will be cases where this is blatantly untrue. In short, by establishing such a high threshold for defining a "contact", the application significantly increases the capacity of a user to be able to identify who their exposure was, simply by reflecting on who they have been in contact with for 15 continuous minutes over the past two-week period. The consent that the user gives is predicated on the anonymous nature of the application; if this is not the case, disclosure is unlawful.

The Government of Canada acknowledges this risk,[135] but attempts to dismiss it by claiming in small communities, public identification of a person as COVID-positive is possible through other means, which "may be more likely to publicly identify COVID-positive individuals than the app itself".[136]

This attempt to hand-wave away concerns of identifiability is improper and unjustified. The fact that identifiability is possible through other routes (such as small town rumours or local community knowledge) does not negate or detract from finding a "serious possibility"[137] of identification as a result of this disclosure from the COVID Alert application, should a user have only one or two persons who meet these stringent criteria. Furthermore, contrary to the Government of Canada's assertions, these concerns are not limited to small communities, as larger cities, far more than rural communities, are being urged to reduce their exposures outside of the home.[138] And further still, a recurring theme throughout this analysis is that a positive diagnosis of communicable disease is health information, which ought to bear a higher standard of protection, given its sensitive nature, as raised under the preceding section. The Government of Canada fails to address this element at all in their privacy assessment of COVID Alert.

2.2.2.3 Data which are identifiable by the actions of malicious third parties' linkages

Finally, the role of malicious third parties in rendering information collected by COVID Alert identifiable ought to be considered. These concerns are important to address because of the significant cybersecurity risks. The Government of Canada is not the only actor with an interest in pursuing personal information. The Herjavic Group's 2019 official report projects that cybercrime will double from $3 trillion in 2015 to $6 trillion by 2021, and claims that cybercrime

---

[135] COVID Alert Assessment, *supra* note 35, states "if an individual has had contact with a very limited number of individuals in the past 14 days, it's possible that the user who receives the notification may be able to associate it with an individual".

[136] *Ibid* at footnote 7.

[137] *Gordon*, *supra* note 71 and *Canada Info Comm*, *supra* note 72.

[138] Government of Canada, "Coronavirus disease (COVID-19): Measures to reduce COVID-19 in your community", *Canada.ca*, (9 October 2020), online.

poses the "greatest threat to every company in the world, and one of the biggest problems with mankind".[139] When these sorts of applications are considered, developed and distributed, the impacts of malicious third-parties must be considered.

By their nature, RPIs are designed to not be identifiable; they are intended to be public information and are openly disclosed to third-party devices.[140] The Government of Canada claims that even if an RPI were to be intercepted by a user with malicious intent, that actor would be unable to connect that RPI to any other person without significant effort, and additional information – in this case, a TEK. TEKs are almost always stored locally, on the device, and as mentioned above, are only released to the server when the user has tested positive, and with the consent of said user. A significant reason the application utilizes this combination of TEKs and RPIs is for anonymization – as per the Government of Canada, "to reduce the risk of re-identification to near zero".[141] That said, note the usage of the term "near-zero"; anonymization is not perfect.[142] The Government of Canada does acknowledge the possibility of a process called a "linkage attack", but claims the risk of such an attack is low.[143]

Linkage attacks involve a third-party connecting, or "linking", anonymized information (in this case RPIs and/or TEKs) to other forms of information available[144] to that third party, thereby rendering anonymized information identifiable.[145] However, the Government of Canada's claims that the risk of such attacks is low does not appear to be supported by the literature, which reports that even sparse datasets can be de-anonymized with relatively minimal effort.[146] Further research has revealed that the use of linkage attacks is not an uncommon means to deanonymize data, including a study which successfully carried out an academic linkage attack of the Joint Canada/United States Survey of Health 2004, by using non-sensitive microdata to link the results to identifiable persons.[147] These studies illustrate that the ability to deanonymize data through linking is improving over time, and health data is not immune to these attacks.

---

[139] Herjavic Group, "2019 Official Annual Cybercrime Report" (2019), Cybersecurity Ventures, at 2, online.

[140] Apple & Google, "Exposure Notification Bluetooth Specification" (April 2020), at p 5, online.

[141] COVID Alert Assessment, *supra* note 35.

[142] Narayanan, A & Shmatikov, V., "Robust De-anonymisation of Large Sparse Datasets" (2008), IEEE Computer Society Conference 111 at 124. This study reported being able to de-anonymise movie ratings of 500,000 Netflix subscribers by cross-referencing the dataset to the IMDB website.

[143] COVID Alert Assessment, *supra* note 35. Note what the Government of Canada refers to as a "linkage attack", authors refer to as "tracking" or "deanonymization" attacks. See Gvily, Y., "Security Analysis of the COVID-19 Contract Tracing Specifications by Apple Inc. and Google Inc." (2020) IACR Preprint at 10-13, online.

[144] Merener, M., "Theoretical Results on De-Anonymization via Linkage Attacks" (2012) 5 Transactions of Data Privacy 377 at 399 states that data used for the linkage attack may be obtained either legally, by skimming data publicly available online, or by hacking or illegal exploitation.

[145] Gvily, *supra* note 143 at 10.

[146] Narayanan & Shmatikov, *supra* note 142.

[147] Merener, *supra* note 144.

Such attacks are not impossible against applications similar to COVID Alert. Deanonymization of data has been shown to be possible with similar, Bluetooth-based contact tracing applications, simply by utilising two different time-location pairs, examining the strength of the received RPI, transmission power, and the location of the third-party attacker's device to infer locations over time.[148] Attackers are then able to target users with reasonable accuracy, by observing who is present at particular inferred locations over a period of time, thereby connecting RPIs to individuals.[149]

Furthermore, if/when a person uploads their TEKs using a PTHA key, the malicious actor would be able to use this identified RPI(s) to track and trace that person's path or route, including potentially the addresses of the user's places of work and/or residence, both of which are "identifiable" under the statute.[150] That said, mitigation of this concern could be accomplished by having the application vary the signal strength, which would throw off the ability of the third-party device from triangulating the device location based off signal strength.[151] It is not clear whether or not COVID Alert utilises this mitigation strategy, as the Government of Canada does not refer to it.

Reidentification of the individual could also be accomplished through a "singling-out" attack, which is far more difficult to mitigate. This process is accomplished by a third-party attacker targeting an individual, bringing a device within close proximity, recording their RPI(s), then stopping the recording; if the target receives a positive diagnosis within the notification window, the published keys allow the attacker to match the known RPI, and single the target out.[152] This attack can also be done at-scale, deploying multiple third-parties, multiple devices, or both.[153] Countermeasures have ben proposed, including requiring a minimum number of devices to be nearby before recording is enabled,[154] but this reduces the application's efficacy.

Furthermore, the Government of Canada's assertions that IP addresses are securely stored,[155] and are only accessible to a small number of government employees bound by security obligations, conveniently ignores the fact that IP addresses are included in the metadata of the TEK codes sent to and from the servers. If a person were to intercept those TEK codes and examine the metadata, they would be able to find IP addresses, and potentially identify the person who

---

[148] Gvily, *supra* note 143 at 11-12.

[149] *Ibid*.

[150] As per the *Privacy Act*, *supra* note 40 at s. 3.

[151] Gvily, *supra* note 143 at 11-12.

[152] *Ibid* at 12.

[153] *Ibid*.

[154] *Ibid*.

[155] Furthermore, this suggests a collection, even if it is the government's assertion that this information is not being actively "collected" *per se*; see *Privacy Act*, *supra* note 40 at s 10(1). The main issue here is with the government's assertion that this information fails to be considered "identifiable".

has tested positive for COVID-19, utilising legally-obtained linkage data.[156] Further, confidence in security and access minimisation does not equate to an impervious database; though CDS may not utilise IP addresses for identifiability, disclosure of this information to a third party who possesses data, or the means to access such data, which is capable of rendering the information identifiable is sufficient to render the information identifiable.[157]

In short, contrary to the arguments raised by the Government of Canada in their privacy assessment, the data collected by this application can, in fact, be considered identifiable under certain circumstances. Data linkages are becoming increasingly sophisticated, and the literature illustrates that there is a demonstrated ability to identify anonymized health data via linking.[158] I would argue that this supports a conclusion there is a "serious possibility" of identification.[159] These concerns are amplified by the highly restrictive methodology utilised by the application in determining if a person is a "contact" thereby posing a significant risk that a person may be identifiable by an application user simply by reflecting on who fits the criteria.

RPIs and TEKs, though theoretically effective at ensuring user privacy, are not infallible, and account must be taken of whether it is possible to link these disclosed data (and/or the associated metadata) with publicly available information, thereby rendering the data identifiable by a third-party with potentially malicious intent.[160] To what extent application programming has integrated some or all of the mitigation measures suggested by the literature[161] is not clear without a deep dive of the application source code, which is outside the scope of this paper, but it does bear mention. If these mitigation measures are not in place, disclosure of TEKs, RPIs, and associated metadata become potentially identifiable via linkage with other available information by third parties, rendering consent for the disclosure invalid, and therefore unlawful.[162] Looking to the future, as technology advances, concerns around linkage will only increase.[163]

3 European Regulatory Framework

Before analysing the existing EU law to determine how and to what extent it may be used as a case study to improve the Canadian legislative framework, it is important to highlight how EU law functions. EU law can be broken down in to two primary forms: Regulations and Directives.

---

[156] OPCC IP Addresses, *supra* note 39 at 5-6.

[157] See *Gordon*, *supra* note 71, at para 43 discusses that when it comes to determining whether information is identifiable, the personal information which is disclosed must be considered in conjunction with other publicly available information.

[158] Merener, *supra* note 144.

[159] *Gordon*, *supra* note 71; *Canada Info Comm*, *supra* note 72.

[160] In accordance with *Gordon*, *supra* note 71 at para 43.

[161] As outlined by Gvily, *supra* note 143 at 12.

[162] As per the *Privacy Act*, *supra* note 40.

[163] von Tigerstrom, *supra* note 20 at 277.

The European Commission defines Regulations as applicable, enforceable and legally binding upon all EU member states upon coming in to force, and need not be adapted or translated in to the national law of a member state.[164] Conversely, EU Directives impose a requirement upon EU member states to adapt measures in the Directive in to national law, thereby achieving the Directive's outcome, but those states are permitted to determine how that outcome is achieved.[165] The resulting trade-off is that the flexibility in how those requirements are met can result in a lack of harmonisation when Directives are in force, as opposed to Regulations.[166]

In the context of privacy and data protection law, the key statute in the EU is the General Data Protection Regulation (GDPR).[167] The GDPR was adopted in 2016, and came in to force May 25, 2018, [168] thereby replacing the preceding 1995 Data Protection Directive.[169] The existence of the GDPR, however, does not preclude Member States from passing their own national laws pertaining to privacy and/or data protection, but any such laws are either repealed or have their scope reduced to the extent to which they are in conflict with enumerated provisions under the GDPR; states may only impose legislation on areas of data protection which are not under the purview of the GDPR.[170] It is also important to note that the GDPR does contain "opening clauses", or derogations which allow one or more national laws to prevail in certain circumstances; therefore, on wholesale consideration, the GDPR, though powerful in its own right, is not the sole authority on data protection, even for EU member states.[171]

It is worth mentioning that there are a number of other legal instruments which purport to regulate some aspect of privacy or data protection, including, but not limited to, the Charter of Fundamental Rights of the European Union,[172] the European Convention on Human Rights,[173] and an array of transnational private regulations. These have varying degrees of applicability to the issue at hand; however, because this paper will focus on what lessons can be learned or what

---

[164] European Commission 'Types of EU Law' (n.d.), online.

[165] *Ibid*.

[166] Kuner, C., Bygrave, L.A., & Docksey, S., (eds), *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford: Oxford University Press, 2020 at 11.

[167] GDPR, *supra* note 89.

[168] European Commission, "Data protection in the EU", *Data protection*, (n.d.), online.

[169] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October 1995 OJ 1995 L 281/31.

[170] Kuner et al., *supra* note 166 at 11.

[171] *Ibid*. Article 49 of the GDPR, *supra* note 89 contains derogations for specific circumstances, and there are other examples besides.

[172] European Union, *Charter of Fundamental Rights of the European Union*, Official Journal of the European Union (2010) 83:53 at 380.

[173] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14* (4 November 1950) ETS 5.

elements can be adapted in improving Canadian privacy law, are considered to be beyond the scope of this paper, and will not be discussed further.

3.1 The GDPR

The GDPR is the predominant form of data protection law in the EU,[174] and is considered to be a "global benchmark in the field".[175] It is important to highlight here the difference between privacy and data protection, as these terms are not the same, and neither are defined directly in the GDPR. The International Association of Privacy Professionals considers privacy to be whether personal information is being appropriately used under the circumstances, whereas data protection is the management of that personal information.[176] The GDPR has illustrated a movement away from protecting privacy alone, and towards imposing broad, overarching requirements for data protection.[177]

It would therefore be incorrect to claim the GDPR is purely privacy law; it extends far beyond this ambit. By its name, the GDPR purports to regulate data protection, which is a means of ensuring privacy, but includes diverse other regulatory requirements, including provisions on automated decision making,[178] data portability,[179] and the right to data erasure,[180] known colloquially as "the right to be forgotten". For the purposes of this paper, however, we will be examining the GDPR through the narrow scope of a means of facilitating and improving the individual's right to privacy, through these data protection requirements, how it achieves this purpose, and what Canada can learn or adapt in its upcoming revisions to its privacy statutes.

The GDPR's purpose is that it "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data".[181] Determining if the GDPR applies requires first determining if the data in question meets the definition of the term "personal data". Note that the GDPR's usage of "personal data" differs from "personally identifiable information" used by Canadian statutes.[182] The GDPR defines personal data under Article 4(1), and the Article 29 working party further clarified by dividing it in to four key parts: (a) information, (b) relating to (c) an identified or

---

[174] Hoofnagle et al., 'The European Union general data protection regulation: what it is and what it means' (2019) 28:1 ICT Law 65 at 66.

[175] Kuner et al., *supra* note 166 at 2.

[176] International Association of Privacy Professionals, "Glossary of Privacy Terms", *Resource Centre*, (nd), online.

[177] GDPR, *supra* note 89 at art. 1.

[178] *Ibid* at art. 22.

[179] *Ibid* at art. 20.

[180] *Ibid* at art. 17.

[181] *Ibid* at art. 1(1)

[182] Whether the difference between information and data has any impact on the definition is unlikely. The functional differences between these two definitions will be analysed in further details in the following section, but for now, it is worth noting that the two definitions are similar, but the definition in the GDPR is broader.

identifiable (d) natural person.[183] Functionally, data which may "relate to an individual, whether the data are public or private, sensitive or non-sensitive, directly or indirectly identify a person, and whether identification is possible now or in the future" are personal data.[184]

This is an extremely broad definition, and this broadness has been upheld and affirmed by the Court of Justice of the European Union (CJEU), that "any information" is intended to capture a wide scope, not just information which is sensitive or private, but all information, including that which is subjective, provided it relates to the data subject, in this case the user of the application.[185] Information which relates to facts pertaining to a person's private life meets this requirement, in nearly any form.[186] That said, considering information which has historically met this definition,[187] it is fair to consider interactions between persons during the course of one's private life, as collected by COVID Alert, would meet this definition under the GDPR.

Moving on to the next step, "relating to", the CJEU also takes a broad interpretation; as per *Nowak*, it is where "the information, by reason of its content, purpose or effect, is linked to a particular person".[188] Given the very nature of a contact tracing application is to link the information to another person, specifically to track who a user interacts with, as well as the communicable disease status of an individual, and the potential for that data to be linked as outlined in the preceding section, it would be fair and reasonable to assume that the information collected by an application such as COVID Alert would meet this criteria.

The following element rings of the Canadian process; that the information be identifiable. In this case, the CJEU has been clearer than the Canadian courts, utilising a flexible approach, arguably more so than that which has been put forth by the Federal Court of Canada. The rule, when reading Article 4(1) in conjunction with recital 26, is that it be possible to "single out", "directly or indirectly" "either by the controller or another person". The CJEU has held that the data in question may be personal data even when the controller cannot link the data to a person without information or assistance from third parties.[189] The issue of identifiability, how it compares to the Canadian regulatory requirements, and how Canada can improve will be put to more thorough analysis in section 4.1 of this thesis.

---

[183] Purtova, N., "The law of everything. Broad concept of personal data and future of EU data protection law" (2018) 10:1 Law, Innovation and Technology 40 at 45-6.

[184] Hoofnagle, *supra* note 174 at 73.

[185] C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994 at para 34. [*Nowak*]

[186] C-141/12 and C-372/12 (Joined Cases) *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* (AG Opinion) [2014] ECLI:EU:C:2013:838 at para 45.

[187] See Kuner et al., *supra* note 166 at 109-110.

[188] *Nowak*, *supra* note 185 at para 35

[189] *Breyer*, *supra* note 128 at para 43.

The "natural person" requirement is fairly straightforward – it precludes these protections from being in force for non-natural persons, such as corporations, but also does not preclude these protections from applying to non-EU residents in EU/EEA nations.[190]

It is important to note the GDPR precludes a few categories of what would otherwise be personal data from applicability. Notably, the EU is not permitted to legislate on matters of member state's national security.[191] Applicability is also excluded for law enforcement,[192], journalistic activities,[193] processing which is of a purely personal or household activity, [194] or for data which pertains to deceased persons.[195]

Having established the data in question is personal data, and therefore under the ambit of the GDPR, an analysis of applicability then flows to whether there is an entity which meets either the definition of a data controller[196] or processor[197] which is processing[198] that personal data. Though there is an enshrined difference in the statute between a controller and a processor, this difference is blurring; functionally, data processors may wish to be considered controllers, as there is a relatively little difference in the attached liability, but data controllers have greater discretion to process data than do data processors.[199] If these definitions are met, the GDPR applies, unless an enumerated exception is met.[200]

4 Improving the Canadian Privacy Framework

The shortcomings of the Canadian federal framework have been acknowledged by the Canadian Privacy Commissioner, who has stated "Canada's laws have unfortunately fallen significantly

---

[190] In accordance with GDPR, *supra* note 89 at art. 3.

[191] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1 at art. 4(2).

[192] GDPR, *supra* note 89 at art. 2(2)(d)

[193] *Ibid* at art. 85. See also generally C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECLI:EU:C:2008:727.

[194] *Ibid* at art. 2(2). See also generally C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596; and C-212/13 *František Ryne v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428.

[195] GDPR, *supra* note 89 at art 2(2)(c)

[196] *Ibid* at art 4(7)

[197] *Ibid* at art 4(8)

[198] *Ibid at* art. 4(2) defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

[199] *Ibid* at arts. 4(7) and 4(8). Data controllers determine the purposes for which and means by which personal data is processed, whereas data processors process data on behalf of a controller. Therefore, processors have less authority than do controllers.

[200] *Ibid.* Some exceptions have been indicated above, as per Article 2, but other exceptions can be found in Article 49, which enshrines derogations in specific circumstances pertaining to transfers of personal data to third countries outside the EU or to other international organisations.

behind those of trading partners in terms of the enforcement of privacy laws" and that "most Canadians believe their privacy rights are not respected by organizations".[201] Serious and significant reforms are imperative to restore Canadian faith in their legal protections, and to hold both private and public actors who violate these laws to account.

This analysis will therefore reflect upon the issues and shortcomings highlighted and discussed under section 2 of this paper, both in respect to the *Privacy* Act, and its interpretation by the Canadian courts. Whether and to what extent these shortcomings can be reduced or corrected by adopting or applying elements of the GDPR or its interpretation by the CJEU as discussed in section 3 of this paper will be considered, with a goal to suggest ways in which the Canadian privacy law framework may become more effective, comprehensive, and clear.

4.1 Improving the Interpretation of "Identifiability"

When considering the differences in terminology between the GDPR and Canadian law, specifically the differences between defining what data constitutes personal information[202] and what can be found to be personal data,[203] a few areas come forward where the Canadian framework could improve. One such area is in the finding of "identifiability of personal information/data. As introduced above, the GDPR imposes a broad consideration of what can be considered personal data, which includes not just sensitive or private information, but potentially all kinds of information, including both subjective and objective information, opinions, and assessments, provided it 'relates to' a data subject – a definition which is also quite broad.[204]

Both definitions rely on identifiability, but in my opinion, this is where the Canadian privacy law framework could improve by adapting elements from the existing EU law, specifically how these terms in the GDPR have been interpreted by the CJEU. The *Privacy Act* does not address or account for linkage attacks, or the role that linking information may have in determining whether a piece of data can be considered identifiable. However, this is not a drawback *per* se, as neither does the GDPR. As mentioned previously, it is somewhat inevitable that some degree of statutory interpretation will be required.

However, statutory interpretation is where the issues arise. As analysed under section 2 of this paper, Canadian courts have not clearly and consistently interpreted what identifiability entails, or precludes information being considered identifiable as a result of illegally obtained linking

---

[201] Office of the Privacy Commissioner of Canada, "2018-2019 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*", *Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy* (10 December 2019), online. [OPCC 2018-2019 Annual Report]

[202] As defined in the *Privacy Act*, *supra* note 40 at s 3.

[203] GDPR, *supra* note 89 at art. 4(1)

[204] *Nowak*, *supra* note 185 at 34.

data.[205] The imposition here is that, were a malicious third party to obtain such information, regardless of how that information is obtained, so long as there is a "serious possibility" of identification,[206] the information could be considered under the purview of statute. This test sets the threshold higher than it does in the EU, while simultaneously failing to clearly identify the effect that anonymization has on identifiability. The interpretation of the *Privacy Act* suffers when compared to that of the GDPR, insofar as the identifiability criterion is concerned – the *Privacy Act* does not speak to anonymization, future risks of deanonymization, or how identifiability may be qualified in respect to the potential of legal future deanonymization, due to the progression and improvement of available technology.

Compare this to the approach taken in interpretation of the GDPR; the Article 29 working party has stipulated its views on what anonymization means under the statute - "data is not identifiable, ie anonymous, only when anonymization is irreversible."[207] This accounts for the fact that a piece of data which is anonymous when it is collected can become personal data at some later point, by no other means than by the evolution of technology – we cannot comprehend what technology will be capable of 5, 10, or 100 years from today.

Furthermore, the EU framework does have a means of addressing the issues with linkage attacks and other cybersecurity vulnerabilities. Like one of the interpretations of "identifiability" made by Canadian courts,[208] the GDPR has been interpreted and explained as taking an approach which can find data to be identifiable even if the controller cannot link the data in question to a particular person without additional information or assistance from other sources.[209] However, in the EU, interpretation of this provision is entirely more clear; though the information need not be in the control of the data controller, the CJEU has been clear that the linking information in question must be able to be obtained legally.[210]

These concerns around identifiability must be addressed in Canadian law; if the courts cannot or will not clarify[211] this interpretation and provide Canadians with these protections, then the

---

[205] *Gordon*, *supra* note 71 at para 43 speaks to the role that "publicly available" information may play in rendering an IP address identifiable, but did not explicitly preclude illegally obtained information from being used to "identify" an individual. Consider, for example, illegally hacked or leaked information which is then made publicly available; it is unclear whether this information could be used to find information identifiable.

[206] As per *Gordon*, *supra* note 71 and *Canada Info Comm*, *supra* note 72.

[207] *Purtova*, *supra* note 183 at 48

[208] Recall the threshold for determining identifiability of personal information is where the information poses a "serious possibility that an individual could be identified through the use of that information**, alone or in combination with other available information**" (emphasis added) as per *Gordon*, *supra* note 71.

[209] GDPR, *supra* note 89 at art. 4(1) and Recital 26

[210] *Breyer*, *supra* note 189 at 40-49.

[211] Amendments to the *Privacy Act*, *supra* note 40, may be required to address or rectify these issues, including misinterpretations or interpretative shortcomings. For a court to interpret a statutory provision, a party must

responsibility falls to Parliament with the upcoming revisions to the *Privacy Act* to include provisions on linkage, and clarifying how such data may be obtained to render information identifiable.[212] Given the rapid nature of technological advancements, it would be preferable for the responsibility to fall with the courts, which can adapt to changing circumstances and adjust the interpretation more easily than Parliament can revise a statute. However, if the Courts are unwilling to do so, statutory revisions must be forward looking – consideration must be given as to what happens when anonymized data becomes identifiable as a result of changing or improving technology.

4.1.1 Clarifying IP Addresses as Identifiable Personal Information

As has been discussed under section 2 of this paper, there is conflicting information from the Government of Canada as to whether IP addresses are personal information. On one hand, the Government has admitted IP addresses *are* personal information,[213] and since 2013, the Privacy Commissioner of Canada has supported this conclusion.[214] However, in the context of COVID Alert, the Government of Canada seems to claim that IP addresses collected in the operation of the application are not identifiable, stating that "CDS does not have the technical means to connect an IP address or API token to an individual smartphone and/or individual".

This lack of clarity is not reflected in European jurisprudence, which has held that IP addresses were personal data because they allow users to be identified[215] and that even dynamic IP addresses are personal information, where the IP address is recorded and the operator of the website is able to lawfully obtain information from an ISP to identify the user.[216]

It is entirely reasonable, especially for government authorities, to conclude that IP addresses are personally identifiable information, and any Government Institution process which collects, processes or stores them ought to be subject to the *Privacy Act*, insofar as that collection, processing and/or storage is concerned. Canadian Courts must update their interpretation of the statute, releasing clear binding jurisprudence holding that IP addresses are, in fact, identifiable. If this is not possible, or the courts are unwilling to do so, then this must be adopted in to statute.

---

either bring a case where interpretation is at issue, appeal such a case to an appellate court, or seek leave to appeal to the Supreme Court of Canada. Courts cannot render judgements in a vacuum without a party bringing such a case before the court. If no such case is brought, it falls to government to rectify these issues by statute.

[212] Note this is in the best interests of the Government of Canada, and not just for COVID Alert; information which is illegally obtained, and which renders anonymized data identifiable under the current framework can potentially open up the government to a statutory violation.

[213] GoC Privacy Policy, *supra* note 39 at note 3.

[214] OPCC IP Addresses, *supra* note 39 at 7 suggests that IP addresses, though not always identifiable on their own *per se*, can be a starting point for identifying an individual, especially as technology progresses.

[215] C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL* [2011] EU:C:2011:771 at para 51.

[216] *Breyer*, *supra* note 189 at paras 45-49.

4.2 Eliminating the Private/Public Enterprise Split

The split between private and public enterprise in regards to Canadian Privacy law adds to this lack of clarity. The particulars of the public/private split have been raised and discussed under section 2 of this paper, but it bears examination in the context of COVID Alert, and comparison to the European approach. As introduced above, the GDPR does not stipulate different regulatory regimes for the private versus public sectors. Instead, it serves as a single, overarching, statute which applies where there is processing of personal data.[217]

That is not to say that the GDPR applies perfectly evenly to both private and public sectors in all cases; there are articles contained therein that carve out exceptions or state explicit applicability to either the public or private sector. [218] However, the base applicability of the GDPR is not differentiated by whether the controller/processor is a public or private entity.

Considering COVID Alert was developed and released by the federal government; it is fair to assume that it falls under the exclusive purview of the *Privacy Act*. Such seems to be the conclusion of the Federal government, which does not mention PIPEDA anywhere in its published resources on COVID Alert. However, the application does not operate in a vacuum; the private sector could be tied in through one of two possible avenues. Firstly, as described above, it interfaces with the GAOS layer – software developed by, and ultimately owned by – the private sector. Secondly, consider that data is transmitted over cellular towers owned and operated by (largely[219]) the private sector. Which actor is responsible for a breach of privacy resulting from malfunctioning of the application? What happens when responsibility for the breach is jointly borne by both the private and public sector? It seems fundamentally unfair that when both sectors are responsible for a breach, that they would be subjected to very different sanctions. Having different rules for the public and private sector does not facilitate accountability.

The current Canadian privacy regime is unprepared for issues which cross this public/private divide. The Privacy Commissioner of Canada has acknowledged that "the law has not properly contemplated privacy protection in the context of public-private partnerships" and the Canadian legal framework "is simply not up to protecting our rights in a digital environment".[220]

---

[217] GDPR, *supra* note 89 at art. 1.

[218] *Ibid* at art. 27, for example, stipulates where processing of personal data (including offering of goods or services, or monitoring behaviour of data subjects within the EU) is done in the EU by a controller or processor not established in the EU, the controller or processor shall designate in writing a representative in the EU. This requirement, as per Article 27(2)(b) does not apply to public authorities or bodies.

[219] Most Canadian cellular telecommunications are owned and operated by the private sector – one significant exception is Saskatchewan, in which telecommunications are owned and operated by the public crown corporation SaskTel. See Canadian Radio-television and Telecommunications Commission, "Communication Service Providers in Canada", *crtc.gc.ca*, (27 June 2016), online.

[220] Office of the Privacy Commissioner of Canada, "2019-2020 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*", *Privacy in a* Pandemic, (8 October 2020), online. [OPCC 2019-2020 Annual Report]

The reality is that the while this may have been an effective form of legislating privacy in Canada decades ago, in the current age of rapid technological advancement, it no longer is. However, the unique challenges Canada faces in the form of federalism (discussed under section 2.1.3 of this paper), entirely eliminating this distinction may well be impossible. If this is, indeed, the case, then it falls to Parliament to ensure that both the private and public sector are held accountable to equal extents.

This accountability issue is also related to the subject of the following section, the woefully inadequate and unequal enforcement regimes of Canadian privacy law which can be levied against the public and private sectors. Though complete elimination of the public/private split may not be feasible, due to federalism, the public and private sectors ought to at least be held to the same standard. This will ensure a fair, level, regulatory playing field, a more coherent, understandable regulatory regime, improve the accountability of the public sector, improve public confidence that entities will act in compliance with statute, and help to bring Canadian privacy law in to line with the international norm.

4.3 Improved Enforcement Mechanisms

A thorough analysis of enforcement mechanisms is outside this paper's scope, but analysis of the Canadian privacy law framework would be incomplete without acknowledging the inadequacies of Canadian enforcement mechanisms. For example, consider the quanta available under the GDPR. For less severe infringements,[221] a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year (whichever amount is greater) can be levied.[222] For those infringements which go against the core principles of the GDPR,[223] a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year (whichever amount is greater) can be levied.[224] Whether or not these fines under the GDPR will be effective deterrents remains to be seen, but one thing is clear – they far outstrip any current financial penalties under Canadian legislation.

The current Canadian privacy legislative framework is exceptionally weak when it comes to enforcement. The only fine that can be levied under the *Privacy Act* is for persons who obstruct the Privacy Commissioner.[225] There are no other statutory pecuniary punishments enshrined in statute should the government contravene a section thereof.

---

[221] As per the GDPR, *supra* note 89 at Art. 83(4)(a) through (c), infringement of some or all of the provisions contained in Articles 8, 11, 25-39, 41(4), 42, and/or 43 may be subject to this fine.

[222] *Ibid* at Art. 83(4).

[223] *Ibid* at Art. 83(5)(a) through (e), infringement of some or all of the provisions contained in Articles 5-7, 9, 12-22, 44-49, 58(1) and (2), and any obligation under Chapter IX may be subject to this fine.

[224] *Ibid* at Art. 83(5).

[225] See the *Privacy Act*, *supra* note 40 at s. 68(2)

Though PIPEDA does stipulate fines for a breach, such fines are only for the breach of specific, enumerated provisions not of particular relevance to this analysis,[226] and the quanta of which is still relatively paltry.[227] Infringement of other sections, such as the duty of the Commissioner to maintain confidentiality,[228] are not subject to fines or other penalties under PIPEDA. Provincial privacy statutes may contain lesser or greater fines, but these statutes do not apply to the federal level, as is discussed in the preceding sections. This discord points to a fundamental inequity in expectations for the private versus that of the public sector.

This is not to suggest that statutory fines are the only enforcement option available. Complaints may be submitted to the Privacy Commissioner of Canada,[229] criminal charges can be laid pursuant to the *Criminal Code*,[230] or civil litigation may be levied against a party under an available cause of action.[231] However, this does not mean the current enforcement framework is adequate; there is a serious need for improvement of enforcement mechanisms, and this has been a recurrent theme of the Canadian Privacy Commissioner's annual reports to Parliament.[232]

4.4 Bottom-up vs Top-down Regulation

The GDPR in general tends to impose bottom-up legal, regulatory processes; for example, requiring concepts like data protection by design and by default, data controllers are expected to incorporate the principles of data protection (an important element of privacy) throughout the entire technological process.[233] This ensures data controllers consider and integrate privacy considerations in every step of the process of developing technology.[234] It instills and requires a risk-based approach to privacy and data protection, accounting for every element from cost, the state of technology, risks, potential impacts, with the ultimate goal of ensuring that personal data is afforded the highest practical degree of protection.[235]

---

[226] Including provisions on retention of information (PIPEDA, *supra* note 41 at s 8(8)), breaches of security safeguards (s 10.2) the reporting and notification thereof (s 10.3), maintenance of records for breaches (s 27.1(1)).

[227] *Ibid* at s 28(b), the maximum possible fine is $100,000. Consider the economies of scale at play; in 2019, Google's revenue was $162 billion USD (see Alphabet, Inc., "Alphabet Announces Fourth Quarter and Fiscal Year 2019 Results", (3 February 2020), online.) A fine of $100,000 can easily be construed by corporations whose profits measure in the billions as simply 'the cost of doing business'.

[228] As required under s. 20(1) of PIPEDA, *supra* note 41.

[229] Pursuant to the *Privacy Act*, *supra* note 40 at s 29, or PIPEDA, *supra* note 41 at s 11.

[230] *Criminal Code*, RSC 1985, c C-46 at s 342.1(1) pertains to unauthorized uses of a computer, rendering hacking a criminal offense.

[231] For example, negligence. Note certain provinces may also establish a tort of a breach of privacy. See *The Privacy Act*, RSS 1978, c P-24 at s 2.

[232] OPCC 2019-2020 Annual Report, *supra* note 220.

[233] GDPR, *supra* note 89 at Art. 25.

[234] Information Commissioners Office, "Data protection by design and default", *Guide to the General Data Protection Regulation* (nd), online.

[235] GDPR, *supra* note 89 at Art 25.

Contrast this to the Canadian regulatory regime. In the public sector, there is no requirement for integrated protections of a person's personally identifiable information. Under PIPEDA, the situation is even worse; this statute relies heavily on self-regulation and self-reporting[236] to ensure the statute is being complied with. The Canadian Privacy Commissioner has indicated that there is a need to move away from self-regulation, but no real change has yet materialised.[237]

Related to this concept is the idea of collection limitation. Though analysis of the efficacy of COVID Alert is outside of the scope of this paper, it is important to briefly note that over-collection of personal data, or collection for no purpose other than its collection, is improper, in accordance with the principle of data minimisation.[238] Therefore, a contact tracing application which fails in its purpose (effective tracing of persons exposed to communicable disease, and/or the control of the spread of disease) will fail this standard, in that it is not collecting personal data for a legitimate purpose, and is therefore in contravention with this principle. It would stand to reason that integration of concepts such as this would only bolster the Canadian privacy law framework.

Summarily, it follows that any technological development, whether by the public or private sector, ought to incorporate a bottom-up regulatory framework, and account for collection limitation. This shifts the onus to the developer, holding them to a high degree of accountability, while ensuring controls are qualified to the relative risk and state of current and future technology, thereby avoiding unnecessary over-correction or constant revisions to statute – what is in accordance with data protection by design will change over time, as technology and implementation costs change. This would also help to level the regulatory requirements, partly solving the above-analysed issue in respect to the private/public split, and poor enforcement mechanisms under the current Canadian privacy framework.

5 Conclusion

Privacy legislation in Canada is showing its age and is no longer fit for purpose. The development and implementation of contact tracing applications, in response to the COVID-19 pandemic, can be used as a case study to further illustrate this inadequacy. This partly stems from a lack of clarity as to what constitutes personally identifiable information, partly from the out-of-date and confusing approach to splitting statutes by whether the data are being collected, processed, or stored by a public or private entity, but also stems from a generally outdated overall approach to privacy regulation.

---

[236] Office of the Privacy Commissioner of Canada, "PIPEDA Self-Assessment Tool", *PIPEDA Compliance* (12 December 2012), online.

[237] OPCC 2018-2019 Annual Report, *supra* note 201.

[238] von Tigerstrom, *supra* note 20 at 250.

Considerations for reviewing, revising and updating Canadian privacy legislation were underway before COVID-19 emerged, and the pandemic has reinforced just how seriously reforms are needed. This thesis is intended to prove that the federal government need not rewrite that which is already written – a comprehensive and clearer framework already exists in Europe.

Adapting the EU's approach to identifiability clarifies what constitutes a breach insofar as linkage attacks are concerned – if a person has legal access to linking information, the information is identifiable; illegal access to linking information is irrelevant. Furthermore, information ought only to be truly considered "anonymized" when it is irreversible, accounting not just for the possibility of identification at the time of the collection, processing or storage, but an ongoing consideration, accounting for the advancement of technology over time.

Furthermore, eliminating the public/private divide in Canadian privacy law would improve the consistency of application of privacy law tenets, reduce confusion when the private and public sectors intersect, and make for a more understandable and confidence-inspiring regulatory regime. Should federalism prevent this homologation, then at the very least, public and private sectors should be held to the same standards, and in those rare, special circumstances where public sectors require an exemption, such should be assessed on a case-by-case basis, and only included where absolutely necessary (as is done under the GDPR's regulatory regime).

Finally, as has been suggested by the Canadian Privacy Commissioner,[239] a wholesale shift in approach is necessary to modernise Canadian privacy law. For too long, the approach has been to ensure the public sector follows a bare minimum standard and to leave industry to self-regulate. Such an approach is far from inspiring the confidence of the populous – industry recurrently demonstrated that they can hardly be trusted to self-regulate. By adopting the EU's approach to bottom-up integration discussed in the previous section, privacy law can be comprehensive and rigorous without becoming too prescriptive.

Notwithstanding these numerous, significant advantages, it is important to note the major issue any substantive Canadian regulatory process must face – federalism. As mentioned above, the nature of sections 91 and 92 of the *Constitution Act*,[240] the fact that privacy is not enshrined as either a federal or provincial jurisdiction, means a comprehensive resolution, or even an attempt to improve these issues, may be impossible. There are limits to what can be done, what Ottawa can stipulate, or force provinces to adopt, but in any case, at least some changes must be made.

[239] Office of the Privacy Commissioner of Canada, "Modernizing federal privacy laws to better protect Canadians: Remarks at a federal Access to Information and Privacy community meeting", *Speech by Daniel Therrien, Privacy Commissioner of Canada*, (1 June, 2020), online.

[240] *Constitution Act, supra* note 45.

Table of References

Abdurasulov, A., "Coronavirus: Why has Turkmenistan reported no cases?" *BBC News,* (7 April 2020), online: <https://www.bbc.com/news/world-asia-52186521>.

Aitken, P., "North Korea's Kim Jong Un again claims country has no coronavirus cases", *Fox News,* (10 October 2020), online: <https://www.foxnews.com/world/north-korea-kim-jong-un-coronavirus-icbm>.

Albert, R. "The Difficulty of Constitutional Amendment in Canada" (2015) 53:1 AB Law Reform 85.

Alphabet, Inc., "Alphabet Announces Fourth Quarter and Fiscal Year 2019 Results", (3 February 2020), online: <https://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf?cache=79552b8#:~:text=%E2%80%9CIn%202019%20we%20again%20delivered,Officer%20of%20Alphabet%20and%20Google>.

Apple & Google, "Exposure Notification Bluetooth Specification" (April 2020), online: https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf

Bland, S., "Reflections on the History of Contact Tracing", *O'Neill Institute for National & Global Health Law,* (13 July 2020), online: <https://oneill.law.georgetown.edu/reflections-on-the-history-of-contact-tracing/>.

C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596.

C-141/12 and C-372/12 (Joined Cases) *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* (AG Opinion) [2014] ECLI:EU:C:2013:838.

C-212/13 *František Ryne v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428.

C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994.

C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.

C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL* [2011] EU:C:2011:771.

C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECLI:EU:C:2008:727.

Canada (Information Commissioner) v *Canada (Minister of Public Safety and Emergency Preparedness)* 2019 FC 1279.

Canada (Information Commissioner) v *Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157.

Canada (Minister of Public Safety and Emergency Preparedness) v Kahlon, 2005 FC 1000.

Canada (Minister of Public Safety and Emergency Preparedness) v Lin, 2011 FC 431.

Canadian Charter of Rights and Freedoms, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Canadian Radio-television and Telecommunications Commission, "Communication Service Providers in Canada", *crtc.gc.ca*, (27 June 2016), online: <https://crtc.gc.ca/eng/comm/services.htm>.

Centers for Disease Control and Prevention, "Measles Transmission", *cdc.gov,* (5 November 2020), online: <https://www.cdc.gov/measles/transmission.html>.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1.

Council of Europe, "Digital Solutions to Fight COVID-19" (October 2020) *2020 Data Protection Report.*

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14* (4 November 1950) ETS 5.

Constitution Act, 1867, 30 & 31 Victoria, c 3 (UK).

Criminal Code, RSC 1985, c C-46.

Dagg v Canada (Minister of Finance) [1997] 2 SCR 403.

Danquah L.O., et al, “Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study” (2019) 19:810, *BMC Infectious Diseases.*

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995 OJ 1995 L 281/31.

Englander v Telus Communications Inc, 2004 FCA 387.

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

European Centre for Disease Prevention and Control, “ECDC Scientific Advice: Systematic review on the incubation and infectiousness/shedding period of communicable diseases in children”, (June 2016) ECDC.

European Commission, “Data protection in the EU”, *Data protection,* (nd), online: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>.

European Commission “Types of EU Law” (nd), online: <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en#:~:text=There%20are%20two%20main%20types%20of%20EU%20law%20%E2%80%93%20primary%20and%20secondary>.

European Union, *Charter of Fundamental Rights of the European Union*, Official Journal of the European Union (2010) 83:53 at 380.

Gordon v *Canada (Minister of Health)*, 2008 FC 258.

Government of Canada, “Coronavirus disease (COVID-19): Measures to reduce COVID-19 in your community”, *Canada.ca,* (9 October 2020), online: <https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/prevention-risks/measures-reduce-community.html>.

Government of Canada, “Coronavirus disease (COVID-19): Prevention and risks”, *Canada.ca,* (3 November 2020), online: <https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/prevention-risks.html>.

Government of Canada, *COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment*, (October 2020), online: <https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html>.

Government of Canada, “COVID Alert Privacy Notice (Exposure Notification)” *Public Health Services*, (13 November 2020), online: <https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy.html>.

Government of Canada, “Download COVID Alert Today” *Coronavirus Disease (COVID-19),* (30 October 2020), online: <https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html>.

Government of Canada, “Modernizing Canada’s *Privacy Act*”, *Department of Justice*, (5 June 2020), online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.

Government of Canada, “Privacy” *Canada.ca*, (2 November 2020), online: <https://www.canada.ca/en/transparency/privacy.html>.

Government of Canada, “Treasury Board of Canada Secretariat Organisation”, *Canada.ca*, (27 July 2020), online: <https://www.canada.ca/en/treasury-board-secretariat/corporate/organization.html>.

Gvily, Y., “Security Analysis of the COVID-19 Contract Tracing Specifications by Apple Inc. and Google Inc.” (2020) IACR Preprint, online: <https://eprint.iacr.org/2020/428.pdf>.

Herjavic Group, “2019 Official Annual Cybercrime Report” (2019), Cybersecurity Ventures, at 2, online: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>.

Hernandez-Orallo, E., et al. “Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19” (2020) 8 *IEEE Access* 99083.

HIV.gov, “How is HIV transmitted?”, *HIV Basics*, (24 June 2019), online: <https://www.hiv.gov/hiv-basics/overview/about-hiv-and-aids/how-is-hiv-transmitted#:~:text=Contact%20between%20brken%20skin%2C%20wounds,is%20not%20spread%20through%20saliva>.

Hoofnagle et al., ‘The European Union general data protection regulation: what it is and what it means’ (2019) 28:1 ICT Law 65.

Information Commissioners Office, “Data protection by design and default”, *Guide to the General Data Protection Regulation*, online: <https://ico.org.uk/for-organisations/ guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accoun-tability-and-governance/data-protection-by-design-and-default/#:~:text=The%20GDPR%20requires%20you%20to,by%20design%20and%20by%20default'.&text=Previously%20known%20as%20'privacy%20by,part%20of%20data%20protection%20law>.

International Association of Privacy Professionals, “Glossary of Privacy Terms”, *Resource Centre*, (nd), online: <https://iapp.org/resources/glossary/>.

Jackman, M, “Constitutional Jurisdiction Over Health in Canada” (2000) 8 Health Law Journal 95.

Kiernan, S., & DeVita, M., “Travel Restrictions on China due to COVID-19”, *Think Global Health*, (6 April 2020), online: <https://www.thinkglobalhealth.org/article/travel-restrictions-china-due-covid-19>.

Kuner, C., Bygrave, L.A., & Docksey, S., (eds), *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford: Oxford University Press, 2020.

Ma, C., & da Silva, E., “Supreme Court of Canada hears carbon tax constitutionality appeals, *Miller Thompson News*, (25 September 2020), online: <https://www.millerthomson.com/en/publications/communiques-and-updates/transportation-logistics-communique/september-25-2020-transportation/supreme-court-of-canada-hears-carbon-tax-constitutionality-appeals/>.

Merener, M., “Theoretical Results on De-Anonymization via Linkage Attacks” (2012) 5 Transactions of Data Privacy 377.

Narayanan, A & Shmatikov, V., “Robust De-anonymisation of Large Sparse Datasets” (2008), IEEE Computer Society 111.

National Oceanic and Atmospheric Administration, “The Global Positioning System”, *GPS.GOV*, (22 April 2020), online: <https://www.gps.gov/systems/gps/>.

Noroozi, E., “Which countries have not reported any coronavirus cases” *Al-Jazeera* (14 September 2020), online: < https://www.aljazeera.com/news/2020/09/14/which-countries-have-not-reported-any-coronavirus-cases/>.

Norton Rose Fulbright, “Contact tracing apps: A new world for data privacy”, *Data Protection Report*, (October 2020), online: <https://www.nortonrosefulbright.com/en-kr/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy>.

O’Carroll, C., & Weisensee, N., “Tourism to North Korea suspended amid China coronavirus concerns: operator”, *NK News* (21 January 2020), online: <https://www.nknews.org/2020/01/tourism-suspended-to-north-korea-amid-china-coronavirus-concerns-ypt/?t=1579741235759>.

Office of Information Technology, “Find Your MAC Address”, *UCInet* (20 October 2020), online: <https://www.oit.uci.edu/mobile/registration/find-your-mac-address/>.

Office of the Privacy Commissioner of Canada, “2018-2019 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*”, *Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy* (10 December 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/>.

Office of the Privacy Commissioner of Canada, “2019-2020 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*”, *Privacy in a Pandemic*, (8 October 2020), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/>.

Office of the Privacy Commissioner of Canada, "Modernizing federal privacy laws to better protect Canadians: Remarks at a federal Access to Information and Privacy community meeting", *Speech by Daniel Therrien, Privacy Commissioner of Canada*, (1 June, 2020) , online: <https://priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200309/>.

Office of the Privacy Commissioner of Canada, "PIPEDA in Brief", *The Personal Information Protection and Electronic Documents Act*, (7 June 2020), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>.

Office of the Privacy Commissioner of Canada, "PIPEDA Self-Assessment Tool", *PIPEDA Compliance* (12 December 2012), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/pipeda_sa_tool_200807/>.

Office of the Privacy Commissioner of Canada, "Provincial and territorial privacy laws and oversight", *About the OPC*, (11 June 2020), online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/>.

Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You", *Technology Analysis Branch*, (May 2013).

Ohio State University, "Contact tracing's long, turbulent history holds lessons for COVID-19", (20 July 2020), online: <https://news.osu.edu/contact-tracings-long-turbulent-history-holds-lessons-for-covid-19/>.

Ontario (Attorney General) v Pascoe, [2002] O.J. No. 4300 (CA).

Owusu, P.N., "Digital technology applications for contact tracing: the new promise for COVID-19 and beyond?" (2020) 5:36, *Global Health Research and Policy.*

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

Pierucci, A., & Walter, J., "Joint Statement on Digital Contact Tracing (28 April 2020) *Council of Europe*, online: <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>.

Privacy Act, RSC 1985, c P-21.

Purtova, N., "The law of everything. Broad concept of personal data and future of EU data protection law" (2018) 10:1 Law, Innovation and Technology 40.

R v Spencer, 2014 SCC 43.

Radio New Zealand, "Solomon Islands has first case of COVID-19", *RNZ* (3 October 2020), online: <https://www.rnz.co.nz/international/pacific-news/427539/solomon-islands-has-first-case-of-covid-19>.

Reference re legislative powers as to regulation and control of aeronautics in Canada, [1930] S.C.R. 663.

The Privacy Act, RSS 1978, c P-24.

Union of Canadian Correctional Officers - Syndicat des Agents Correctionnels du Canada - CSN (UCCO-SACC-CSN) v *Canada (Attorney General)* 2016 FC 1289.

Union of Correctionnel [*sic*] *Officers* v *Canada (Attorney General)*, 2019 FCA 212.

United Nations World Tourism Organisation, "100% of Global Destinations Now Have COVID-19 Travel Restrictions, UNWTO Reports", (28 April, 2020), online: <https://www.unwto.org/news/covid-19-travel-restrictions>.

von Tigerstrom, B. *Information and Privacy Law in Canada*, (Toronto: Irwin Law, 2020).

Weisman, S., "What is a distributed denial of service attack (DDoS) and what can you do about them?" *Norton Emerging Threats*, (23 July 2020), online: <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html>.

Wells et al., "Impact of international travel and border control measures on the global spread of the novel 2019 coronavirus outbreak" (2020) 117:13 PNAS 7504.

World Health Organisation, "Contact Tracing", *WHO Newsroom*, (9 May 2017), online: <https://www.who.int/news-room/q-a-detail/contact-tracing>.

World Health Organisation, *Novel Coronavirus (2019 nCoV) Situation Report 1* (Geneva: World Health Organisation, 2020) , online: <https://www.who.int/docs/default-source/coronavirus/situation-reports/20200121-sitrep-1-2019-ncov.pdf?sfvrsn=20a99c10_4>.

World Health Organisation, *Statement on the second meeting of the IHR (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)* (Geneva: World Health Organisation, 2020), online: <https://www.who.int/news-room/detail/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov)>.