PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC
285 McLeod Street, Suite 200, Ottawa, ON K2P 1A1

9 September 2020

Mr. Claude Doucet
Secretary General
Canadian Radio-television and
Telecommunications Commission
Ottawa, ON K1A 0N2

VIA GC KEY

Dear Mr. Doucet,

Re: ***Part 1 Application Regarding "COVID Alert" App, "ABTraceTogether" App and Related Matters***

The Public Interest Advocacy Centre (PIAC) hereby files a Part 1 application requesting specific Commission action (as specified in the Application) in relation the "COVID Alert" App, the "ABTraceTogether" App, and regarding Canadian telecommunications service providers' involvement in the operation of these contact-tracing apps. In particular, this Application seeks Commission guidance on privacy rules for potential government requests to TSPs to provide subscriber information associated with the use of COVID Alert, ABTraceTogether and any potential future similar tracing technologies.

This Application is PIAC's second regarding pandemic contact-tracing, however, it is not a re-submission of the first Application but now is based on actual assessment of these deployed apps, now used by many Canadians. As such, we request that the Commission now deal substantively with the Application.

Sincerely,

John Lawford,
Counsel to PIAC

cc Named respondent TSPs
Stephen Millington, CRTC
Daniel Therrien, Privacy Commissioner of Canada
Jill Clayton, Information and Privacy Commissioner of Alberta
Patricia Kosseim, Information and Privacy Commissioner of Ontario

BEFORE THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION

IN THE MATTER OF AN APPLICATION UNDER THE *TELECOMMUNICATIONS ACT* BY

THE PUBLIC INTEREST ADVOCACY CENTRE

PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

(APPLICANT)

and

Bell Canada; Bell Mobility Inc.; Bragg Communications Incorporated, carrying on business as Eastlink; Canadian Communication Systems Alliance (CCSA), Cogeco Communications Inc., Canadian Wireless Telecommunications Association (CWTA); Distributel Communications Limited, Freedom Mobile Inc.; Ice Wireless Inc.; Independent Telecommunications Providers Association (ITPA), Iristel Inc., Quebecor Media Inc., on behalf of Videotron Ltd. (Videotron); Rogers Communications Inc. (Rogers); Saskatchewan Telecommunications Holding Corporation, operating as SaskTel (SaskTel); Shaw Communications Inc. (Shaw); TBaytel; Teksavvy Solutions Inc., Telus Communications Company (TELUS); Xplornet Communications Inc.

(RESPONDENTS)

REGARDING "COVID ALERT" APP, "ABTRACETOGETHER" APP AND RELATED MATTERS

9 September 2020

Table of Contents

1.0 Introduction 3
2.0 Public Health and the Purpose of this Application 7
3.0 The Parties 8
4.0 The Facts 9
4.1 COVID Alert App 9
4.2 ABTraceTogether 13
5.0 IP Addresses and Privacy 14
5.1 IP Addresses and the Law 15
5.1.1 IP Addresses in Canadian Case Law 15
5.1.2 IP Addresses and CRTC Decisions 15
5.2 IP Addresses as Described to the Public in the COVID Alert App 17
5.2.1 IP Addresses as Described in the COVID Alert Sign-up Process 23
5.3 Phone Number collection as Described in the ABTraceTogether Sign-up 26
6.0 Law: Privacy Under the Telecommunications Act 28
6.1 History of Customer Confidential Information, Telephone Numbers and Subscriber Information under the Telecommunications Act 29
6.2 The Role of Customer Consent in the Disclosure of Customer Confidential Information 33
7.0 Public Order Exceptions to Consent under Present Telecommunications Privacy Law . 36
8.0 Public Health App Exception to Explicit Consumer Consent to Release CCI 38
9.0 CONCLUSION AND REQUESTED RELIEF 44
10.0 APPENDIX 1: A “Privacy-First” Canadian Public Policy Approach to Digital Contact Tracing Technology (“DCTT”) Related to COVID-19 & Future Pandemics 46

1.0 INTRODUCTION

1. The Public Interest Advocacy Centre (PIAC) files this Application under the *Telecommunications Act*[1] and pursuant to Part 1 the CRTC *Rules of Practice and Procedure*[2] regarding digital contact tracing technologies, and in particular, the Government of Canada's ("federal government") pandemic contact-tracing application ("app") for smartphone wireless devices and known and branded as "COVID Alert" (français: "Alerte COVID") and the Government of the Province of Alberta's app known as "ABTraceTogether" and related matters, namely, potential and actual actions by all major Canadian wireless service providers ("WSPs") to identify Internet Protocol addresses ("IP addresses") or mobile telephone numbers, by matching them with their subscriber data and potentially providing that matched subscriber information to the federal or any provincial government.

2. As the Commission is well aware, PIAC at an early stage of the pandemic (May 4, 2020), filed a Part 1 Application asking the Commission to inquire into the potential involvement of all Telecommunications Service Providers ("TSPs") in pandemic app deployment.

3. On 17 August 2020, the Commission finally responded to PIAC's initial application in a Letter Decision. The Commission found that the public interest was not best served by appointment of an Inquiry Officer or the issuance of a Notice of Consultation. It noted that:

> […] PIAC's application, as filed, is broad in nature and does not identify a specific activity or action by TSPs in the development or implementation of contact tracing measures such that Commission intervention is warranted at this time. In addition, it does not demonstrate that existing privacy frameworks and protections are insufficient at this time to address the issues it has identified.

4. This new Part 1 Application is now brought, due to revelation of the details of, and the launch of, in particular, the "COVID Alert" app, so that we now are aware of its operation and flaws, and the roles of the TSPs in privacy violations. In short, this Application is specific in reciting the activities and actions of TSPs in contact tracing measures and further, lays bare the lack of existing protections under other existing privacy frameworks and their inability, in any meaningful manner, to control the creation and deployment of DCTTs.

[1] S.C. 1993, c. 38.
[2] SOR/2010-277, s. 22.

5. We respectfully request that the Commission publicly post this new Application, which is in due and proper form, in accordance with its rules of procedure, before making any procedural or substantive rulings on our application. Should the Commission wish to combine our previous application with this new one, or that we formally withdraw the previous one, or considers the first Application dismissed, or that this one is somehow inappropriate, we signal that whatever the procedural approach, refusing to post this, our new application, is not acceptable.

6. Finally, we note that the Commission stated at the close of its Letter Decision of 17 August 2020, that it would be willing to reconsider the issue:

> Should the factual circumstances change or should indications arise that TSPs are participating – or contemplating participating – in contact tracing measures, the Commission may reconsider whether to inquire into these activities in order to determine what, if any, additional measures should be taken. As part of its monitoring efforts, the Commission will continue to communicate with the OPC.

7. We therefore submit that it is not appropriate to dismiss this new Application on the basis that it already has been considered, or that we are somehow abusing the Commission’s process. We reject those potential objections both on the basis of the above openness of the Commission to reconsider the issue and on the basis that we now have indeed information on TSP involvement in contact-tracing measures, as detailed below.

8. We also attach as Appendix 1, a detailed description of “Digital Contact Tracing Technology” (“DCTT”) in general and of several similar apps and systems, both those developed in Canada and worldwide, including notably COVID Alert and the Government of the Province of Alberta’s “ABTraceTogether” app. Appendix 1 is intended to assist the Commission both with considering our specific allegations regarding COVID Alert and ABTraceTogether but also with regard to any TSP related to a DCTT referred to in this Application. However, where there is a conflict between descriptions of fact or law in Appendix 1 and in this Application, the allegations in this Application are intended to supersede those in Appendix 1.

9. Where this Application makes references to public health policy, law or information; to digital contact tracing technologies in general, operating systems or other technical information or other context-specific information including developments in other jurisdictions, we refer the reader to the particular section of Appendix 1 for more information and PIAC’s views.

10. This application asks the Commission, under its jurisdiction to "promote the privacy of persons" (pursuant to subs. 7(i) of the *Telecommunications Act*, as demanded by s. 47) and a condition of service on TSPs pursuant to s. 24, 24.1 of the *Act*), to require TSPs who are or may be requested to provide subscriber information associated with any IP Address or mobile telephone number information related to COVID-19 apps (COVID Alert, ABTraceTogether or any other DCTT system) to the federal or provincial governments, by:

a) Defining, in the context of any DCTT app (COVID Alert, ABTraceTogether or any other DCTT system), and in particular COVID Alert and ABTraceTogether, the privacy requirements the TSPs must follow under the *Telecommunications Act* and to confirm that these are essentially the same as for confidential customer information developed under the Commission's decisions in relation to telephony;

b) Setting out a test for WSPs to determine whether a request to inquire into IP address resolution (or mobile telephone number lookup) to link to or reveal subscriber information associated with that IP address (or mobile telephone number) for the purposes of any DCTT app (COVID Alert, ABTraceTogether or any other DCTT system) deployed in Canada, without explicit subscriber consent, is permitted, and if so, what test is required to be met to make such a disclosure and what limits, if any, that test might place on disclosure of such information.

c) Specifying particular substantive, transparency and accountability requirements in the above noted test, to encourage compliance with, and enforcement of, the privacy rule determined by the Commission.[3]

11. Our previous contact tracing application also asked the Commission to, as a condition of offering telecommunications service (mobile wireless or Internet access), under the authority of ss. 7, 24, 24.1 and 47 and possibly s. 70 of the *Telecommunications Act*, require all TSPs to:

a) Publicly disclose on the record of this proceeding and to the Commission any steps taken for any government or private interest to facilitate contact tracing;

b) Inquire into any such TSPs' activities related to contact-tracing apps or network-

[3] To this end, and to assist the Commission, PIAC has proposed below such specific particular requirements. These are based on the requirements for promulgation of orders under Ontario's *Emergency Management and Civil Protection Act*, R.S.O. 1990, c. E.9 (the "EMCPA"), as interpreted by the Canadian Civil Liberties' et al.'s Application for Judicial Review of Ontario's O Reg 120/20 Order Under Subsection 7.0.2 (4) Of The Act - Access To Covid-19 Status Information By Specified Persons (the "COVID-19 Status Order").

level facilitation of individual consumer location or other personal or communications details;

c) Require any such TSPs’ activities related to contact tracing respect the confidential customer information rules of the Commission devised for telephony;

d) Prohibit TSPs from using prior consumer consent to location track mobile devices (for example, in “opt-in” marketing programs or other TSP portal or other applications) or to provide databases previously gleaned from these programs to any private or government entities to build, improve or test COVID-19 tracing tools without new, explicit, prior individual consent for this new use or disclosure;

e) Appoint an inquiry officer under subs. 70(1)(a) of the *Telecommunications Act*, to inquire into and report upon contact tracing, as well as to liaise with public health authorities and governments and non-telecom private parties, if necessary;

f) In the alternative, launch a formal Notice of Consultation on the matter.

12. We continue to believe that certain aspects of the previous application remain potentially helpful to the public, to telecommunications providers, to other regulators and to the government (including the Commission) and that it would have been helpful for the Commission to have considered our initial Application in a timely and thorough matter at that time. This may have provided a baseline of rules for consideration by the federal and provincial governments in developing their applications and for the telecommunications industry in responding to such apps and systems. Be that as it may, certain of these older suggestions may be necessary or desirable matters for the Commission to now consider in tandem with our present Application, in particular with regard to any number of new or future DCTT apps or systems.

13. Finally, we note for the Commission that we have communicated this Application to the federal Office of the Privacy Commissioner of Canada, and to the privacy commissioners of Ontario and Alberta, respectively, as the Application may assist these offices in their interactions with the public or with the various governments and app developers, as the case may be. However, we underline that this Application is not a complaint under any of the statutes overseen by those privacy commissioners but rather only a complaint under the Telecommunication Act.

14. However, should the Commission delve deeply into the present Application, it may find that the involvement of these privacy commissioners would assist it. We do not oppose such consultation; however, we vehemently oppose dismissing or suspending this Application on the basis of such other venues – CRTC jurisdiction over telecommunications is plenary and proper.

2.0 PUBLIC HEALTH AND THE PURPOSE OF THIS APPLICATION

15. COVID-19 is an unprecedented and deadly challenge to people worldwide, including people in Canada. PIAC acknowledges the need for significant public health measures to deal with the pandemic and we support the government directives to self-isolate and otherwise physical distance to slow the spread of the virus, along with other measures.

16. PIAC agrees with the internationally and nationally accepted epidemiology of the SARS-CoV-2 virus[4] and accepts that contact-tracing is an important element in the suite of preventive measures societies can put in place, along with testing, physical distancing, hand and face hygiene, including mask-wearing, self-isolation and quarantine practices, as well as societal measures such as societal "shutdowns" and eventual vaccine development.

17. PIAC believes that the present movement to develop COVID-19 apps for contact-tracing primarily is responding to a legitimate public health effort to improve the speed and reach of "manual" contact-tracing of positive or suspected cases and that adoption of such apps, even at levels below 60% of the population,[5] can have meaningful effects on slowing infection spread.

18. We further accept that a trusted contact-tracing app, with significant societal uptake and deployment, could assist in more potentially infected persons getting tested sooner and/or isolating sooner, and that such public acceptance is valuable public health goal.[6]

19. In addition, however, many of these same public health purposes have also been intermingled with possible uses of contact-tracing for government and private sector pandemic control, emergency management, and labour relations, which also consider questions of: quarantine, self-isolation, social (or physical) distancing, essentiality, positive and negative testing and treatment, anti-body testing), but from a labour relations, public order and policing perspective.

4 See, for example, World Health Organization, "Transmission of SARS-CoV-2: implications for infection prevention precautions - Scientific Brief" (9 July 2020); online: https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention-precautions and

5 See Appendix 1, "Adoption of CTA [contact-tracing apps]" at para. 38, and the Oxford study cited therein.

6 We refer the reader to a resource we found useful in understanding the various elements of pandemic response, including possibly an app for contact-tracing, in "What Happens Next? COVID-19 Futures, Explained With Playable Simulations" by Marcel Salathé (epidemiologist) & Nicky Case (art/code), found online, at: https://ncase.me/covid-19/?v=2

20. PIAC wishes therefore to underline that the purpose of this application is not to impede public health contact-tracing for appropriate purposes of public health and that we do not take a position as to the appropriate constitutional or legal or policy limits of public health. However, we do wish to note that the overlap of the effects of using contact-tracing for both public health and pandemic control by government or labour force control or consumer profiling by the private sector raises serious issues that the Commission under its telecommunications oversight jurisdiction must consider not only in depth but in haste.

21. As with the initial application, this Application is based on the principles of transparency, democracy and human rights and accountability. PIAC believes that the value of any DCTT app or system, including in particular COVID Alert and ABTraceTogether, coming at the potential expense of confidentiality and consumer and citizen privacy, must occur in the fairest, most open and transparent manner, non-coercively, non-discriminatorily and only for the intended purpose(s).

22. We also sincerely believe, that the various governments and public health authorities of Canada, rather than trying to evade or deny privacy law, instead should embrace transparency and privacy rules (including those of the *Telecommunications Act* as clarified by the Commission after this Application), so that most Canadians, thus fully informed of their rights and the potential for privacy concerns, and being able to clearly demand that an app or system addresses those concerns, may well adopt such apps and systems *en masse*, in the spirit of mutual aid that reveals their sincere concern for all other Canadians.

23. Without these clear rules, transparency and commitment to rule of law, Canadians will, however, be rightly suspicious of and resist these apps as potential surveillance technologies.

3.0 THE PARTIES

24. The Public Interest Advocacy Centre (PIAC) is a national non-profit organization and registered charity which represents consumer interests – and those of vulnerable consumers in particular – in the provision of important public services.

25. The respondents are major retail mobile wireless service providers (WSPs) or Internet service providers (ISPs); or umbrella groups representing TSP members; inclusively, the “telecommunications service providers” (“TSPs”).

26. While we have named certain of such providers above in the interests of administrative economy and because they serve the vast majority of Canadians – the actual number of TSPs in Canada being very large – we believe that the Commission should decree that this Application's outcome should be applied to all TSPs in Canada. We leave the process for extension of any possible decision to all TSPs to the Commission, whether by show cause proceeding or otherwise; however, we invite and encourage all TSPs to intervene and comment on this proceeding.

27. PIAC's belief that the Commission should provide guidance and rules to all TSPs, not just those named as respondents or to "major" TSPs, is based on our allegation that all TSPs are in the position of having, for their own customers at least, and possibly for other Canadians, confidential customer information and other private information of their subscribers and others, including in particular records of their IP addresses and also possibly mobile telephone numbers, as the result of customer use of DCTTs such as COVID Alert and ABTraceTogether, as detailed below. We will attempt via public posting on our website and through social media to bring this application to the notice of all TSPs in the hopes that they will comment and bring a wider perspective to the Commission but we submit that the Commission posting this application should serve as sufficient notice to all TSPs of the potential for any possible decision to apply to them.

4.0 THE FACTS

4.1 COVID Alert App

28. The COVID Alert "app" was released to the Canadian public on the Apple Store and Google Play on 30 July 2020. Please refer to Appendix 1, paras. 228-277, for more details.

29. This was coincident with the release of privacy analyses of the COVID Alert app by, separately, Health Canada (Government of Canada)[7] and the Office of the Privacy Commissioner of Canada.[8]

30. Shamefully, in our view, Health Canada, in its privacy analysis, stated that it was of the

[7] See: Government of Canada [Health Canada]. "COVID Alert: Exposure notification application privacy assessment" - Canada.ca 2020-07-31, 3:10 PM; online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html

[8] See: Office of the Privacy Commissioner of Canada. "Privacy review of the COVID Alert exposure notification application" - Office of the Privacy Commissioner of Canada 2020-07-31, 1:41 PM; online: https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/

opinion (one which we do not share) that the information created, exchanged and uploaded (see below) by COVID Alert is not personal information and therefore, the federal *Privacy Act* did not apply to the app at all.[9] While expressing exasperation at this conclusion, the federal Privacy Commissioner's office did not contradict this assessment, but rather simply pointed to it as ironic.

31. However, what these two analyses clearly demonstrated was that personal information, that is, IP addresses or mobile telephone numbers (for ABTraceTogether), are associated with certain information (positive diagnosis code) sent over the Internet by the apps. These IP addresses (or mobile telephone number) then can be linked to more personal information in the hands of telecommunications service providers (TSPs) with a simple request for TSP subscriber information associated with the IP address or mobile number. Thus, PIAC contends that the IP addresse and mobile telephone numbers, are indeed "personal information", as they can lead, after a second step of requesting subscriber information from a TSP, to identify at the least the account holder of the Internet connection implicated in the COVID Alert and ABTraceTogether processes.

32. As noted, the TSPs facilitate the transmission, over their connections to the Internet, the transfer of positive diagnosis keys to and from smartphones running the app.[10] This is revealed in the both COVID Alert and ABTraceTogether's descriptions.

33. Dealing first with COVID Alert, each day, on many occasions while the app is installed and the user has agreed to enable notifications at the operating system level (which is a necessary permission to have the app function as intended), the app downloads all positive diagnosis keys previously uploaded by other users testing positive for the virus, from the Health Canada central key server and then processes them to determine if they match daily exposure keys of the app's user. As is made clear in both the Health Canada and OPCC analyses, and in the Google-Apple API specifications, such **downloads of positive diagnosis keys are necessarily associated**

9 We leave aside, in this Application, the equally suspect assertion that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) also did not apply, as private sector companies had "volunteered" or seconded or concluded interchange agreements with private sector companies, such as Shopify or BlackBerry to develop the app or its precursors, and that this studied formal arrangement somehow erased the substantial commercial interest in the development of this particular app and the development of this type of tracing app by governments.

10 For example, the OPCC Review states baldly:

> In addition, system logs will retain users' IP (Internet Protocol) address every time there is a request made to the server (one-time code verification, diagnosis key upload, etc.) for up to three months in normal conditions. In the event of suspicious activity, the system will retain a user's IP (Internet Protocol) address for up to two years. In this scenario, we understand that the relevant system logs may be shared with law enforcement agencies to facilitate an investigation. These security features present a risk of re-identification because, when combined with other information, IP (Internet Protocol) addresses can be used to identify individuals.

with a particular IP address assigned to the smartphone (if the user is connected on the cellular network) or the IP router of the WiFi network to which the smartphone is then connected (if the user is connected on a local WiFi connection).

34. In addition, should the app user test positive for COVID-19 and subsequently receive a one-time upload authorization key from the provincial government health authorities (provided by the federal government), this “positive” user can choose to upload a positive diagnosis key from their smartphone app to the Health Canada. When he or she does so, the **positive diagnosis key is recorded along with the uploading IP address** (again, an IP address from the cellular network if the user’s smartphone is connected on a cellular connection or the IP address assigned to the WiFi router if the user’s smartphone is connected to WiFi) used at that time. See Figure 1 below for details.[11]

[11] In addition, as an explanatory aid for the functioning of the main features of the Apple-Google API underlying the app, we refer the reader to this helpful video explanation by software engineer Hussein Nasser on YouTube: https://www.youtube.com/watch?v=otkKkFrkN88
The video describes the key generation process on the device, how devices upload to a key server in a case where someone is diagnosed as ill, and how other app users download these positive keys to assess if the app user was within a set proximity to anyone diagnosed. This video is clear in explaining what is going on in real-world language, and is helpful for appreciating and understanding what specifically is intended.
The video was published relatively early during the pandemic and prior to the roll-out of COVID Alert and ABTraceTogether, and so there description regarding a system level “patch” or “update” to the Apple or Android operating systems, which is not what has occurred (as noted, the processing happens only in these apps and we do not suggest it happens in the operating system of smartphones). In addition, there may been some minor changes in how the protocol operates, however, to our knowledge, the API generally and the process of key generation/exchange (explaining which is the purpose of this video) remains fundamentally the same.

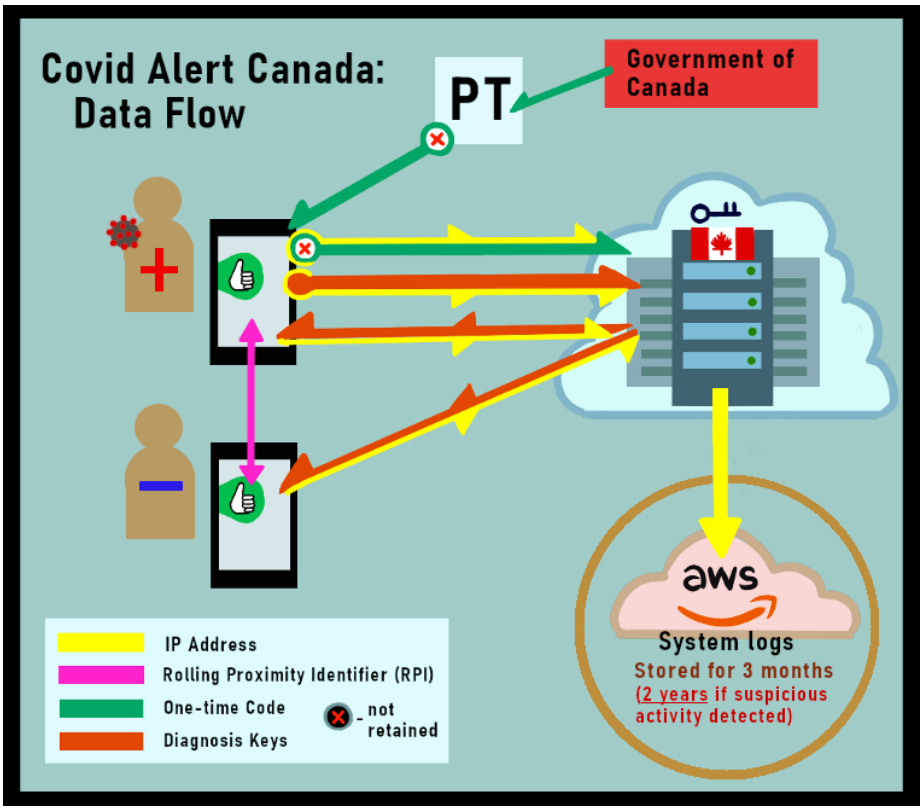


Figure 1: How IP addresses are associated with diagnosis codes under COVID Alert
Source: PIAC

35. This means that contrary to the assertions from the TSPs in response to our initial Application of 4 April 2020 that they are not involved in the functioning of COVID Alert, that they are in fact key to the operation of the system. Without the transmission or uploading and downloading of positive diagnosis codes (which, to be sent over the Internet must originate on an IP address and thus can be associated with that IP address), COVID Alert would not work.

36. TSPs keep logs of IP addresses and which IP addresses were assigned to which of their subscribers, with time and date stamps.[12]

37. TSPs can be asked by the federal government to reveal the names of subscribers associated with positive diagnosis keys, if the government provides the IP address and time associated with the positive diagnosis key upload, to which the government does have access via server logs.[13] This means the government can obtain, with a simple request, and with reasonable

[12] See description of IP address assignment in *R.* v. *Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at paras. 21-26.
[13] It is unclear on the Health Canada or OPCC privacy assessments if the Key Server stores IP addresses associated along with diagnosis keys; however, it is clear that such associated IP addresses are kept on the AWS servers for at least 3 months, and therefore are available to at least the federal government, which contracts with AWS.

certainty, the identity of every Canadian testing positive for COVID-19 who has used the app and reported this positive status.

38. This "IP address leak" also permits the government to identify all Canadians actively using the COVID Alert app (*i.e.*, those who have downloaded the daily diagnosis keys of positive users, but who have not yet uploaded their positive diagnosis, should they be or become infected). That is, the government also can find out the identities of all active users of COVID Alert.

4.2 ABTraceTogether

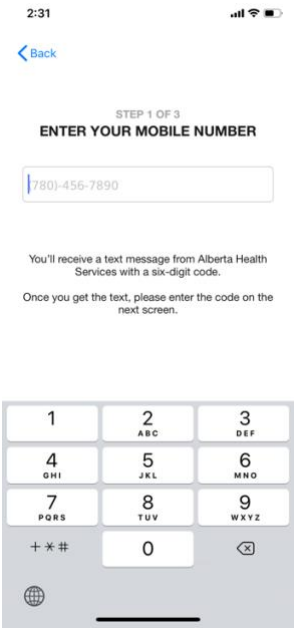
39. The Alberta government also can find out the identities of all users of ABTraceTogether who choose to self-report as COVID-19 positive, as the app uses the Internet connection of the app to transmit data to the central server (for, at the least, positive diagnosis key upload, if not for positive key downloads)[14], by requesting this information from TSPs, based on government and media reports of the functioning of the ABTraceTogether app and the PIA of the Alberta Privacy Commissioner[15].

40. It does not appear that ABTraceTogether, however, permits downloads of positive keys for matching to the device of that apps users; rather, upon a positive diagnosis being reported to Alberta Health, those officials instead contact-trace manually to contact potentially exposed persons. This means that the Alberta government could not, from the IP addresses in ABTraceTogether, obtain the identities of all active users of the app from various TSPs.

41. The ABTraceTogether app, however, to facilitate the manual contact step, specifically seeks user consent to obtain a **mobile telephone number** during the sign-up process. See screenshot below from this part of the ABTraceTogether installation/sign-up process:

[14] *Ibid*., see the "information flow diagram" detailed at para. 22 (which describes user "upload contact logs" and that Alberta Health "receives data" – both presumably via the Internet) and para. 25, which states: "Information uploaded to the server from a user's smartphone …" and see paras. 26 and 27 which speak of logs being "sent" to the central server in Montreal and "uploaded" by the user.

[15] Office of the Information and Privacy Commissioner of Alberta. "ABTraceTogether Privacy Impact Assessment Review Report" - Alberta Health and Alberta Health Services File 015714 (July 2020); online: https://www.oipc.ab.ca/media/1089098/Report_ABTraceTogether_PIA_Review_Jun2020.pdf .



42. Rather than waiting and hoping, as with the COVID Alert app, to obtain this information from a user of the COVID Alert app, (who, after a positive test and even after uploading digital keys confirming his or her COVID-19 status, is still only encouraged to contact (Ontario, as of the date of this Application) public health authorities), it appears that when the user of the ABTraceTogether app takes the step of informing Alberta via the app of his or her positive status, that their mobile number is immediately used by Alberta Health to begin the process of contact-tracing, without again requesting consent. More importantly, this now provides Alberta Health with the mobile number of a “positive” user and Alberta Health is now potentially able to approach TSPs to request other confidential customer information from the TSP in relation to the mobile telephone number (for example, name, service address, billing address, and calling records).

43. Of course, the government also has a list of all mobile telephone numbers of all users of ABTraceTogether. Thus, in effect it also has a key to knowing the identities of all app users.

44. Finally, we note that the Alberta government has committed to transition ABTraceTogether app users and records to the COVID Alert app. See Appendix 1, para. 207, for details.

5.0 IP ADDRESSES AND PRIVACY

45. IP addresses have been consistently found by courts and accepted by the CRTC as being linkable to uniquely private information that allows vast and deep intrusion into the personal lives of Canadians. Courts and tribunals have therefore developed strong requirements for the

protection of, and serious procedural requirements for access to, IP addresses.

5.1 IP Addresses and the Law

5.1.1 IP Addresses in Canadian Case Law

46. The Supreme Court of Canada, in *R* v *Spencer*, 2014 SCC 43, found that a request under PIPEDA's regime for exceptions to consent in subs. 7(3)(c.1)(ii) of that *Act* did not authorize a warrantless request for subscriber data based upon a provided IP address.

47. *R* v *Spencer* fully accepts that subscriber information identifies individuals "by tending to link particular kinds of information to identifiable individuals," therefore implicating "privacy interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information."[16]

48. Furthermore, the court characterized the police's disclosure request in that case as a "request to link a given IP address to subscriber information," which was "in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities."[17]

49. *Spencer*, in a criminal search context, confirmed the very high standard for access to TSP-held subscriber information enabled by a request to link it to a known IP address. In short, such a search requires a warrant.

5.1.2 IP Addresses and CRTC Decisions

50. The Commission has considered the privacy implications of IP addresses in the past and has consistently treated them as highly personal information under the *Telecommunications Act* and in a legal and a policy sense as well.

51. For example, in the context of deep packet inspection, the Commission considered the possibility of TSPs using specific IP addresses of subscribers to inquire into subscriber uses of their Internet connections, in relation especially to high-volume users suspected of using file sharing software, on the supposition that some of such use might potentially violate copyright or otherwise misuse network resources.

[16] R v Spencer, 2014 SCC 43, para 47.
[17] R v Spencer, 2014 SCC 43, para 50.

52. In October 2009, the CRTC released its enforceable guidelines for Internet traffic management practices (ITMPs); Telecom Regulatory Policy 2009-657 set out guidelines for how ISPs must comply with transparency and non-discrimination requirements. In the consultation process, consumer groups warned that without additional safeguards for personal information derived through ITMP technologies, such info "could be collected, stored, and potentially used for purposes other than traffic management without notification and consent."[18] In particular, "parties acknowledged that DPI technologies can be used to access and manage a variety of user information flowing over the ISPs' networks."[19]

53. In TRP CRTC 2009-657, the CRTC's analysis of IMTP-related privacy concerns included a reference to a previous decision, Telecom Decision CRTC 2006-15, as am.,[20] in which "the Commission considered that protecting the privacy of telecommunications service customers was increasingly important due to the advent of new technologies and the emergence of electronic commerce, which enable information to be more easily processed, rearranged, and exchanged."[21] The privacy analysis in TD CRTC 2006-15 also recognized that the CRTC must take a proactive role in protecting the privacy interests of customers, and not rely solely on PIPEDA, as "the Commission considers that market forces, even buttressed by the provisions of the PIPED Act, are unlikely to sufficiently protect the privacy interests of customers in a forborne environment."[22] The CRTC thus saw fit to impose "a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services."[23]

54. In fulfilment of this higher standard, the CRTC in TRP 2009-657 directed all primary ISPs to not use or disclose personal information collected in ITMPs (that is, IP addresses) for other purposes. Additionally, primary ISPs' service contracts with secondary ISPs must also include requirements, as a condition of providing wholesale services, that the latter not use or disclose personal information (including IP addresses) for purposes other than permitted traffic shaping by ITMPs as outlined in that decision.

[18] *Review of the Internet traffic management practices of Internet service providers* (21 October 2009), 2009-657 at para 97, online: https://crtc.gc.ca/eng/archive/2009/2009-657.htm.
[19] *Ibid,* at para 99.
[20] See Telecom Decision 2006-15, as amended by the Governor in Council's *Order Varying Telecom Decision CRTC 2006-15*, P.C. 2007-532, 4 April 2007 (modified Telecom Decision 2006-15).
[21] *Ibid,* at para 101.
[22] *Forbearance from the regulation of retail local exchange services* (6 April 2006) 2006-15 at para 367, online: https://crtc.gc.ca/eng/archive/2006/dt2006-15.htm.
[23] *Supra* note 49, at para 102.

55. In a previous complaint, CRTC 2008-108, Bell Canada was accused of traffic shaping, but the CRTC was satisfied that the traffic shaping was appropriate for addressing congestion on its network during peak periods. The rationale behind this reasoning was that "Bell Canada, as a network operator, is responsible for ensuring that its network is operated effectively and efficiently, and considers that Bell Canada should be able to take measures in this regard."[24] The complaint also proposed that Bell Canada was using Deep Packet Inspection technology to identify the type of data being transferred, the ISP network, and an end-user's intention to acquire specific content, "all of which are personal information under Canadian privacy legislation."[25] In investigating this allegation, the CRTC was satisfied that although Bell is able to examine the source and destination IP address data, there was no evidence on record that this information was collected, used, or disclosed by Bell for any purpose other than traffic management. Nonetheless, the mechanisms of traffic shaping practices show that ISPs are able to track IP addresses in relation to customer activity on its networks. This decision also shows that the Commission was prepared to prohibit use of IP addresses without explicit customer consent, similar to telecommunications law as laid out by the Commission in relation to telephone service (that is, in relation to "Customer Confidential Information" ("CCI") – see discussed below).

5.2 IP Addresses as Described to the Public in the COVID Alert App

56. In the context of the COVID Alert app, there is a possibility that law enforcement may demand access to subscriber information linked to the IP addresses collected by the app. While the IP address implicated in *Spencer* was associated with a residence, the IP addresses involved in COVID Alert is not necessarily tied to a single location. However, the court in *Spencer* suggests the distinction is insignificant; the court stated that "the location where the activity occurs is secondary to the nature of the activity itself… Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, **via smartphones, or portable devices**."[26]

57. Additionally, *Spencer* characterizes the subject matter of the search as "the identity of a subscriber whose Internet connection is linked to particular, **monitored Internet activity**." [emphasis added].[27] In the context of COVID Alert, the "monitored Internet activity" could be the

[24] *The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service* (20 November 2008) 2008-108 at para 28, online: https://crtc.gc.ca/eng/archive/2008/dt2008-108.htm.
[25] *Ibid*, at para 78.
[26] R v Spencer, 2014 SCC 43, para 37.
[27] R v Spencer, 2014 SCC 43, para 33.

users’ diagnosis keys and temporary codes, depending on the extent to which the government actually monitors such activity.

58. We maintain that possible government requests to link IP addresses of positive COVID-19 tested individuals who used the COVID Alert app and chose to upload their status is very similar to access in a criminal search context. We also maintain that Canadians have a reasonable expectation of privacy that in using the app they will not be individually identified or identifiable, with or without a secondary government request to an ISP to match subscriber data and their IP address.

59. One possible question that the government or TSPs may seek to answer differently from how we have just answered it in the COVID Alert context is the uploading user’s reasonable expectation of privacy. It could be argued that the app user, having been asked for explicit consent to upload diagnosis keys in an app installation, reasonably consented to any government use of that status.

60. We argue not, for the simple reason that the reasonable contemplation of uploading a positive diagnosis key would be for the purpose of protecting public health, and it would not be in the reasonable contemplation of users of the app to think that this socially-conscious step would also amount to permission to the government to discover and possibly use and disclosure the individual user’s personal infection status (possibly in ways that would greatly prejudice him or her). Quite reasonably, the individual app user would not, logically, see how knowledge of their individual identity or infection status could assist with the public health response if the app worked as described to the public.

61. We believe that all of the public-facing descriptions of the app, from the install process; through public government communications; commitments made in the app descriptions and in statements to the media; all support the idea that Canadians will not, in any circumstances, be individually identified by the app.

62. For example, the Prime Minister’s Office of Canada on June 18, 2020, announcing COVID Alert app, stated in a press release, in regards to privacy, that:

> Use of the app will be voluntary. If someone tests positive for COVID-19, a health care provider will give them a unique temporary code, so they can upload their status ***anonymously*** to a national network. Other users who have downloaded the app and come in contact with that person will be notified, through the app, that they may have been exposed to the virus. The app will also provide users with information on steps they

> can take to keep themselves and others safe, and we are working with the provinces and territories so they can customize public health information based on their own jurisdiction. [Emphasis added.]
>
> The Canadian Digital Service is leading the development of the app, in collaboration with the Ontario Digital Service and building upon technology developed by Shopify volunteers. The app will undergo a security review by BlackBerry. It incorporates Bluetooth technology provided by Apple and Google to anonymously record instances where users have come into close contact. To protect confidentiality and privacy, **the app *will not disclose the identity of users*. *This information*** will never be shared with any other entity, will not be stored by the app, and ***will never leave the user's phone***. No personal information is collected by the app, and it does not track the user's location to ensure the privacy of all Canadians. [Emphasis added.]

63. On the date of public release of the COVID Alert app, the Rt. Hon. Justin Trudeau, Prime Minister of Canada, made a speech in the following terms to announce the launch of the app:

> "Here's how it works.
>
> The app will let you know if you've been in contact with someone who has the app and has tested positive for COVID-19.
>
> If that's the case, it will then encourage you to call your provincial health services for guidance on what to do.
>
> I want to be clear: this app isn't mandatory—it's completely voluntary to download and to use.
>
> And ***it doesn't collect*** your name, your address, your geolocation, ***or any other personal information***.
>
> I've downloaded the app this morning, and I encourage you to do the same.
>
> The more people use it, the better it can trace and therefore slow the spread of the virus.
>
> In fact, health experts say that if enough people sign up, this app can help prevent future outbreaks of COVID-19 in Canada.
>
> I know that Premier Ford will have more to say about this first made-in-Ontario system, but I want to thank him for his partnership in getting this program up and running."[28] [Emphasis added.]

64. Likewise, the Government of Ontario, in announcing the app was ready for download,

28 PMO, "Prime Minister's remarks on COVID-19 measures and the launch of the COVID Alert national application", (July 31, 2020); online: https://pm.gc.ca/en/news/speeches/2020/07/31/prime-ministers-remarks-covid-19-measures-and-launch-covid-alert-national

issued a press release that made the following statements,[29] asserting that no personal information was shared, four times in the document:

> The COVID Alert app uses Bluetooth technology to detect when users are near each other. If a user tests positive for COVID-19, *they can choose to let other users know* ***without sharing any personal information***. Ontarians who receive an exposure alert can then get tested and take action to help keep themselves, their families, and their friends from spreading COVID-19 throughout the community. The app ***does not collect personal information*** **or health data**, and does not know or track the location, name, address, or contacts of any user.
>
> […]
>
> The app supports the efforts of public health units, allowing the province to quickly test, trace and isolate cases of COVID-19 to stop the spread of the virus and prepare for any potential outbreaks — ***without sharing any personal information***.
>
> […]
>
> - ***COVID Alert does not collect any personal information***, health information, or location data. It uses Bluetooth technology to send out encrypted codes to other nearby app users and was built using the Apple/Google framework for exposure notification to ensure that it leverages global best practices to protect privacy.
>
> [Emphasis added].

65. These statements, to an average Canadian, reasonably would create the impression that a user's identity would not be discoverable with a simple request to their ISP to undercover it. These statements, in particular with regard to those statements regarding uploading a positive test result, such as in the federal government's June 18, 2020 statement, in effect convey the impression that such positive status could not be linked back to any individual, by any method (e.g., "so they can upload their status anonymously to a national network"). Worse, the common sense reading of the above clearly implies that such linking of a positive result to an individual would be impossible. Note the words "[t]his information", which antecedent would normally be read as referring to "the identity of users", is stated to "never leave the user's phone."

66. As seen from Figure 1 above and confirmed in the descriptions of the COVID Alert app in

[29] Ontario, Office of the Premier, New Release: "COVID Alert Available for Download Beginning Today - Privacy-First, Made-in-Ontario App Notifies Users of Potential Exposure to COVID-19" (31 July 2020); online: https://news.ontario.ca/opo/en/2020/07/covid-alert-available-for-download-beginning-today.html

the Health Canada and OPCC assessments, this is plainly false. The information, meaning positive diagnosis keys (and also the download of all others' positive keys), plainly DOES leave the phones of the persons with positive tests who have used the app then gone through the process to "voluntarily" upload the positive diagnosis key. Again, statements such as those above that reasonably appear to guarantee anonymity of such positive upload key transmission information (or download of others' positive keys) ignore the simple process of matching TSP subscriber information to IP address associated with the positive diagnosis keys.

67. Lest it be thought that this is simply political "overselling" of the app's supposed privacy respect, we note in fairness that the OPCC in its assessment of the Health Canada self-assessment (which claimed "anonymity" for users), flagged this IP address issue and said:

> We note, however, that there are situations where the risk is higher, even if still low due to the adoption of strong safeguards. For instance, IP (Internet Protocol) addresses accompany attempts to verify one-time codes to the server. The server retains the user's IP (Internet Protocol) address for 60 minutes if the one-time code is not valid; this retention is meant to help prevent fraudulent uses of one-time codes. In addition, system logs will retain users' IP (Internet Protocol) address every time there is a request made to the server (one-time code verification, diagnosis key upload, etc.) for up to three months in normal conditions. In the event of suspicious activity, the system will retain a user's IP (Internet Protocol) address for up to two years. In this scenario, we understand that the relevant system logs may be shared with law enforcement agencies to facilitate an investigation. These security features present a risk of re-identification because, when combined with other information, IP (Internet Protocol) addresses can be used to identify individuals. But, again, due to the adoption of strong safeguards, we believe the risk of identification is low. The Government of Canada indicated to our Office that access to these logs is restricted to authorized users who are bound by security obligations to protect this information and not to access or use it for nefarious purposes.[30] [Emphasis added.]

68. Unfortunately, the OPCC did not go the extra step to consider that the government itself might take the IP addresses and go to the TSPs to match them with subscriber data.

[30] See: Office of the Privacy Commissioner of Canada. "Privacy review of the COVID Alert exposure notification application" - Office of the Privacy Commissioner of Canada 2020-07-31, 1:41 PM; under heading "De-identification"; online: https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/

69. Even more interesting and ultimately far more misleading, was the Health Canada privacy assessment’s statement of the processing of IP addresses by COVID Alert:

> The *IP address accompanies any request made to the key server* (e.g., when a user chooses to upload their random codes, or enters their one-time code). *However, the IP address is not intentionally "sent" by the app. It accompanies the request* ***naturally****: IP addresses are metadata required as part of the underlying internet protocol that powers data transmission over the Internet; without this, the app and the server would not be able to communicate.* In other words*, IP addresses accompany all requests made to the server (one-time code generation, one-time code verification, diagnosis key upload, etc.).* In most cases, the IP is not of the phone in particular, but of a wireless router or is dynamically assigned by a cellular network carrier. Few people have static IPs that are permanently associable to them, due to the limited number of IPv4 IP addresses. In sending that information, the IP accompanies the request, as with any request sent over the internet.
> In the event the one-time code is not valid, the user's IP address is retained at the key server level for a rolling window of sixty minutes. After eight consecutive invalid attempts from the same IP, the IP is blocked for sixty minutes. The associated IP address is deleted from the system sixty minutes after the last invalid attempt to verify a one-time code.
> [NB: CDS is considering removing this server-level blocking in favour of infrastructure-level firewall rate limiting (described below)].
> IP addresses are stored in access logs on the AWS server, which is separate from the key server, for 3 months for all logs, and up to 24 months for those implicated in a security investigation, for cyber security systems to adequately understand, monitor, and respond to attacks against a system and for the secure and reliable operation of the service.
> Furthermore, IP addresses are not used by CDS to identify the source in any way, and they are not associated with any other data element in the server. The IP addresses are collected for security purposes. They are not used by the CDS-operated system to try to identify the source. IP addresses may be disclosed to law enforcement in the event a malicious actor attempted to gain, or gained, access to the server where they are stored. They would be deleted along with other data once the exposure notification system is shut down (i.e., once the pandemic is declared over), unless they are being retained for a security investigation.
> CDS does not have the technical means to connect an IP address or API token to an individual smartphone and/or individual. API tokens are only associated with PT systems integrating with the key server to obtain one-time codes.
> Regarding IP addresses, technically, this would require either sophisticated analysis (beyond CDS's capabilities), or access to the and subscriber lists of Internet service providers (not within CDS's ability to access or compel).[31] [Emphasis added.]

70. These paragraphs are notable as they: a) fail to mention the potential for the government in general, if not CDS or Health Canada in particular, to approach the TSPs with a view to

[31] See: Government of Canada [Health Canada]. “COVID Alert: Exposure notification application privacy assessment” - Canada.ca 2020-07-31, 3:10 PM; online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html

matching IP addresses and subscriber information; and b) provides a textbook example of misdirection and overdetailed bafflegab to confuse readers and lead them away from posing the question in a).

71. Without expending too much effort to dispel this attempt to assuage citizen concerns, we simply note that:

- There is nothing “natural” in the Internet; IP addresses are indeed required under the “internet protocol” to route packets to the right destination on the network; however, the decision of whether and how to log IP addresses thereafter is a decision of the network programmers as well as the decision to associate IP addresses with other information transmitted or kept in databases;
- The discussion of dynamically-assigned or static IP addresses is irrelevant as TSPs maintain logs of which IP addresses (even dynamic ones) are assigned to which subscribers when;
- The discussion of incorrect one-time code entry and one hour IP retention on the key server does not affect the more permanent (3-24 month) retention of IP addresses associated with positive diagnosis keys on the AWS server;
- While the section detailing the AWS server logs where IP addresses are retained for 3 months (24 months if a “security issue” (undefined) is identified) suggests that the IP logs will only be inquired into for security investigations, but this is not so limited by law or any public government promise;
- Finally, while this Health Canada self-assessment does states that: “Regarding IP addresses, technically, this would require either sophisticated analysis (beyond CDS's capabilities), *or access to the and subscriber lists of Internet service providers (not within CDS's ability to access or compel)*” [emphasis added], the last part of this phrase, while perhaps true due to CDS’s limited mandate, does NOT preclude another arm of the federal government from seeking “to access or compel” the “Internet service providers” to deliver subscriber lists corresponding to IP addresses. Thus, this last statement is highly misleading, as it implies a small, largely unknown part of the federal government (CDS) would not be competent to make disclosure requests but presents the specific “inability” of CDS as a pan-governmental inability. This is a false implication; the federal government, specifically another part such as the RCMP, Canada Border Services, other immigration, policing or security forces or even Health Canada, could most certainly seek TSP cooperation to identify IP addresses.

72. In conclusion, the clear risk of access to subscriber information via presentation of the stored IP addresses is obfuscated in the both the federal government’s and Ontario government’s public statements.

5.2.1 IP Addresses as Described in the COVID Alert Sign-up Process

73. We also detail here the sign-up process for the COVID Alert app with screenshots taken

of that process. This process also supports a reasonable Canadian’s reasonable perception that the app would not lead to their personal identification, unless the user were actively attempting to hack the system. During the sign-up process, none of the main, mandatory screens detailing the general descriptions of the app’s functioning, the positive diagnosis key uploads, or positive key downloads, or of use of the Internet, suggest any risk whatever of the possible identification of the user, but rather appear to reassure the user at several stages that this either cannot, or will not, happen.

74. Statements such as these are commonplace in the main sign-up screens:

> “Your privacy is protected
> COVID Alert **does not use GPS** or track your location.
> It has **no way of knowing**:
> - Your location.
> - Your name or address.
> - Your phone’s contacts.
> - Your health information.
> - The health information of anyone you’re near.”
>
> […]
> “The server only gets the codes. It does not get any information about the person.”

75. Only by accessing optional additional screenshots in the sign-up process at the screen titled: “The app will now ask your permission” under the submenu “Learn more about privacy” (which is not mandatory to view to proceed to give the app permission to start working) can the prospective user find the “Privacy Policy”. We note that for a normal iPhone 11 Pro display at normal resolution, on the screen titled: “The app will now ask your permission”, the link to “Learn more about privacy” is not visible unless the user scrolls right to the bottom of this screen and that there is no textual clue that this important information is sub-linked “below the fold” of this screen (however, this information can also later be found (after actually installing the app) under the “About COVID Alert” heading in the main menu (itself available only after calling it up)).

76. These screens are reproduced below, with red outline emphasis added by us, as they appeared during sign-up with an iPhone 11 Pro on 6 August 2020:

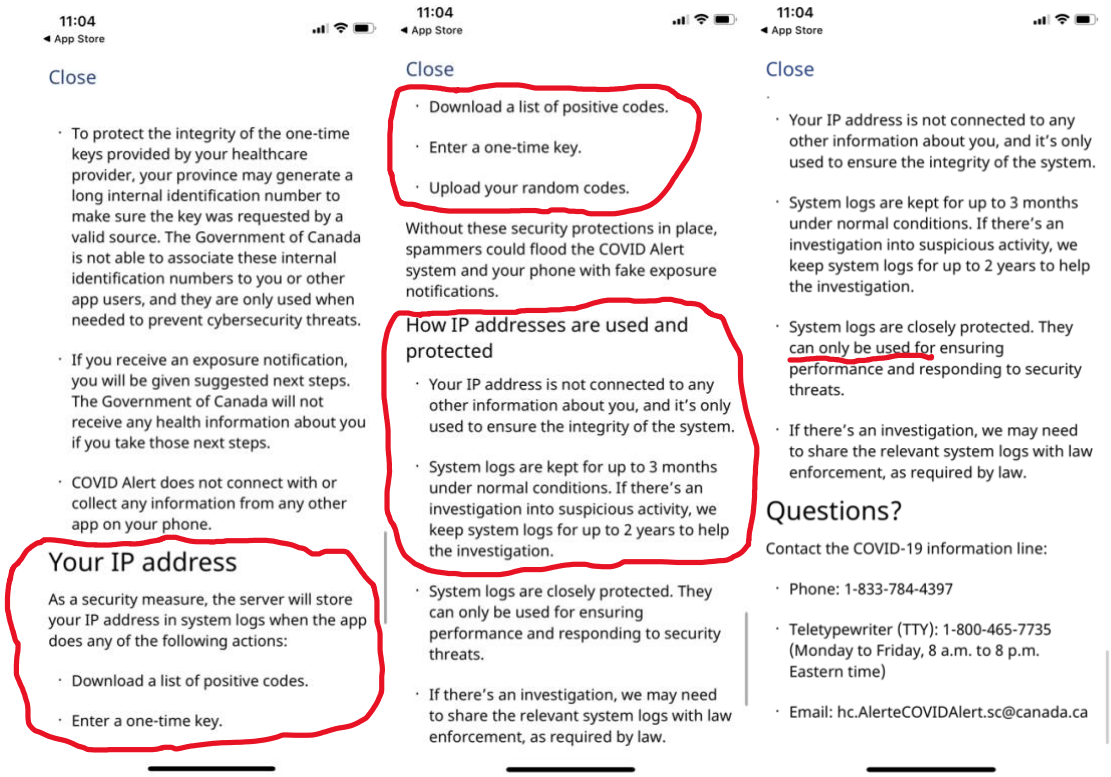


Figure 2: Screenshots of "How IP addresses are used and protected" in COVID Alert sign-up process
Source: PIAC

77. Despite thus hiding the Privacy Policy during sign-up, an intrepid and suspicious user could have found, in the relatively long Privacy Policy, the relevant screenshots regarding the precise issue of "How IP addresses are used and protected" in COVID Alert sign-up process. The entire set of sign-up process screenshots is reproduced in Appendix 1, at Appendix A of that document.

78. It is particularly worth noting that nowhere in the app's sign-up process is there any direct or indirect reference to even the possibility of a secondary government request to an ISP to match subscriber data and their IP address.

79. This fact, however, makes the statements in the Privacy Policy potentially false and certainly misleading. Statements such as: "Your identity and health status will not be shared with the Government of Canada" are contingent on the Government of Canada never making a request to a TSP to link subscriber information and IP address. The statement: "Your IP address is not connected to any other information about you" is at best misleading, in that the app would not reveal the user's identity by itself but, again, this assertion is contingent on the Government of Canada never making a request to a TSP to link the IP address to subscriber information which

is most certainly “other information about you” (namely, your name, address and account number at your ISP).

80. We assert that a reasonable expectation of privacy in an average Canadian after following the sign-up process and even after exploring the app thoroughly after sign-up, would not be limited to include, based on what is presented, a real sense that, should the Government of Canada seek to make a request to a TSP to link subscriber information and IP address that one’s identity could indeed be revealed. We assert that this revelation should be a requirement of the app.

81. Without such a revelation in the app, we assert it is entirely reasonable for the CRTC to place stringent rules on any government requests to make a request to a TSP to link subscriber information and IP address or to obtain that subscriber information.

82. More importantly, PIAC submits that whatever the assertions made in these sign-up processes and whatever the conclusions of Health Canada’s privacy self-assessment and the review of the Office of the Privacy Commissioner of Canada based on general privacy statutes such as the Privacy Act and PIPEDA, that the *Telecommunications Act* imposes privacy requirements on the potential for revelation of subscriber information (customer confidential information) in relation to IP addresses gathered by COVID Alert or any DCTT.

5.3 Phone Number collection as Described in the ABTraceTogether Sign-up

83. Besides the likely IP Address collection by ABTraceTogether, which concerns are similar to those above for COVID Alert, (minus the additional IP address collection by COVID Alert during download of positive keys step, which ABTraceTogether does not appear to perform), an additional problem with the ABTraceTogether is Alberta’s collection of the mobile phone number without informing users that this number now may enable Alberta Health to request additional information from the user’s relevant TSP.

84. Alberta appears not to have considered that the mobile phone number in itself is a key to obtaining further information about users from TSPs. This likely led the Alberta creators of the app and writers of the privacy policy to focus only on provincial privacy law, and not the requirements of federal law, in particular the telecommunications law decreed by the CRTC over the years in relation to privacy.

85. This disconnect/oversight is manifested by the reliance on telephone number as defined

in Alberta privacy legislation (see below) without realizing that such a datum (the 10 digit standard form telephone number, with area code) allows queries to TSPs to discover more information associated with that number.

86. This may be why the ABTraceTogether privacy policy does not appear to contemplate that a user's mobile phone number is itself "personal information" federally, and, as noted, potentially allows inquires with the user's TSP to determine more information associated with the phone number, such as subscriber name and address, billing and account information, and calling logs.

87. For example, the ABTraceTogether privacy policy (the same as displayed within the app), notes on the following about the collection, use or disclosure of the user's mobile phone number:

> Contact information of individuals receiving a positive diagnosis of COVID-19 will be collected for the purpose of conducting contact-tracing. […]
>
> **Withdrawing Consent**
> You can revoke consent by emailing HiaHelpDesk@gov.ab.ca with the mobile number you registered in the application.
> We will then delete your mobile number and User ID from our server. This renders all data that your phone has exchanged with other phones meaningless, because that data will no longer be associated with you.

88. The ABTracetogether privacy policy further identifies the relevant provincial acts thusly: "This information is collected under sections 20(b), 22(2)(a) & 27(2)(c) of the *Health Information Act* (HIA) and sections 33(a)&(c) & 34(1)(a)(i) of the *Freedom of Information and Protection of Privacy Act* (FOIP)."

89. Under the Alberta *HIA*, "registration information" is defined (as a subcategory of "health information") as including telephone numbers:

> **Interpretation**
> 1(1) In this Act,
> […]
> (k) "health information" means one or both of the following:
> (i) diagnostic, treatment and care information;
> (ii) registration information;
> […]
> (u) "registration information" means information relating to an individual that falls within the following general categories and is more specifically described in the

regulations:

(i) demographic information, including the individual’s personal health number;

(ii) location information;

(iii) telecommunications information;

(iv) residency information;

(v) health service eligibility information;

(vi) billing information, but does not include information that is not written, photographed, recorded or stored in some manner in a record;

[Emphasis added.]

90. “Personal information” definitions under these provincial acts are, understandably, missing, given their purposes and the level of government enacting them and the jurisdictional division of powers between telecommunications (almost exclusively federal) and health care (mostly provincial) and public health (shared, in various ways, between federal and provincial).

91. However, it makes clear that provincial privacy policies applying to provincial (health) privacy acts like ABTraceTogether may inadvertently ignore the federal privacy rules regarding matters like telephone numbers or IP addresses, especially if these telecommunications data elements are treated as simple contact or registration” information under provincial acts, without understanding their potential, in telecommunications law, to potentially identify telephone number users or obtain TSP subscriber information.

6.0 LAW: PRIVACY UNDER THE TELECOMMUNICATIONS ACT

92. The *Telecommunications Act* has policy objectives, including subs. 7(i), which requires the Commission to consider how “to contribute to the protection of the privacy of persons” in its regulation of all aspects of telecommunications.

93. As PIAC has noted in many proceedings involving TSP subscriber and Canadian carrier privacy since, subs. 7(i) requires not only: 1. an analysis in addition to general privacy laws (mainly PIPEDA) but also; 2. that a higher standard of privacy must be met to satisfy the “promotion” of subscriber privacy than that outlined generally for private commerce in the *Personal Information Protection and Electronic Documents Act*.

94. To its credit, and despite recent intense pressure from major telecommunications providers who used to promote high levels of privacy under their telephony general tariffs but now appear to see it as a barrier to behavioural advertising and "surveillance capitalism", the Commission has found on multiple occasions that the privacy policy requirements of the *Telecommunications Act* require an extremely high standard of confidentiality and customer privacy be met.[32]

95. We submit that the same high level of consumer privacy applies to the extent that arguments may be raised that government action, in the telecommunications sphere, only be judged by, or is only governed by, the federal *Privacy Act*, the provincial freedom of information and privacy acts or any sector-specific legislation (such as health information legislation) applying to the provincial or municipal governments in the provinces and territories. In addition, we submit that absent a specific exclusion of the Commission's *Telecommunications Act* jurisdiction in a federal emergency order or statute – of which we are presently unaware of any relevant instances, at least in relation to the federal *Emergencies Act* or *Emergencies Management Act* – that the Commission should similarly interpret subs. 7(i) of the *Telecommunications Act* to require a higher standard of privacy than in particular the *Privacy Act* or any provincial statutes.

96. Therefore, the Commission should set out rules in advance for TSPs regarding possible disclosure of subscriber information or other subscriber data related to either IP addresses or telephone numbers that they may have on subscribers.

6.1 History of Customer Confidential Information, Telephone Numbers and Subscriber Information under the Telecommunications Act

97. Before describing the basis for, and approach to, this possible Commission direction on the limiting effects of federal telecommunications privacy law on DCTTs, and in particular, COVID Alert and ABTraceTogether, it is necessary to understand the history and evolution of "customer confidential information" in the telecommunications context, and in particular, the Commission's treatment of telephone numbers and related subscriber information.

98. The story arguably starts with RCMP warrantless surveillance of Quebec separatists in

[32] See Telecom Decision, *Confidentiality provisions of Canadian carriers* (30 May 2003); online: https://crtc.gc.ca/eng/archive/2003/dt2003-33.htm . See alsoTelecom Decision CRTC 2003-33-1 (11 July 2003); online: https://crtc.gc.ca/eng/archive/2003/dt2003-33-1.htm . More recently, see: Telecom Decision CRTC 2015-462, Public Interest Advocacy Centre and the Consumers' Association of Canada - Application regarding Bell Mobility Inc., Solo Mobile, and Virgin Mobile Canada's use of customer information (20 October 2015) at para. 14. Online: https://crtc.gc.ca/eng/archive/2015/2015-462.pdf

the late 1960s, culminating in the 1970 October Crisis.

99. In part due to such warrantless searches and seizures, the Charter of Rights and Freedoms, promulgated as part of the “patriation” of Canada’s constitution in 1982, included s. 8, the constitutional right of freedom from unauthorized search and seizure.

100. Subsequent to the constitutionalization of at least the search aspect of privacy, the new Telecommunications Act was passed in 1992. It included a policy objective that the Commission not only protect telecommunications users’ privacy but that it “promote” the privacy of persons.

101. This strong statement codified the CRTC (and predecessor regulators) careful protection of unlisted telephone numbers (different from those “public” numbers listed in the “white pages” directories along with name, and address if listed as well) as well as calling records and other account-related information.

102. Once law enforcement was required to seek warrants for searches and seizures, the question arose as to how to execute these in relation to information linked to a known telephone number (to obtain unlisted name and address, calling records etc.). This was increasingly exacerbated by the introduction of competition in the provision of local telephone service, in the wake of the CRTC’s landmark Telecom Decision 94-19, setting out the framework for telephone competition in Canada. In short, even with a warrant, police now needed a way to know even which company had control of a particular telephone number, just to present a warrant.

103. This effort was represented by an initial request by law enforcement in Ontario to obtain this information from Bell Canada, which already had a tariff (General Tariff, Item 10, s. 11.1, also described below, as modified) that described the confidentiality of customer information and which Bell interpreted as including even information on the appropriate telecommunications carrier, as well as the other information held in relation to the number.

104. This impasse led to the Commission’s decision in:

> “Telecom Decision CRTC 91-2, Criminal intelligence service of Ontario - Release of information by Bell Canada, dated 12 February 1991, [in which] the Commission denied an application relating to the release of technical information regarding telecommunications facilities to law enforcement agencies in the absence of prior legal authorization. The Commission concluded that the information in question was "information kept by Bell Canada regarding the customer" within the meaning

of Article 11.1 of Bell Canada's Terms of Service. The Commission also stated the following:

> In the Commission's view, provisions concerning the release of customer information for the purposes of law enforcement must, among other things, strike an appropriate balance between the subscriber's interest in privacy and the public's interest in law enforcement. The Commission considers that the current Article 11.1 strikes the appropriate balance between those interests.”[33]

105. To resolve the impasse, in the late 1999, law enforcement and the major telecommunications service providers worked together on a proposal to allow release of LSPID.

106. Their joint proposal, concluded under the forerunner of the CRTC’s “CISC” technical committee, and embodied in Bell Canada’s proposed Tariff 6479, proposed law enforcement agencies (wider than the police, and including any government agency with quasi-policing powers) access without a warrant and with no other requirement than a request after demonstrating “lawful authority” to regulate in the area or an “active investigation” under that authority (or in order to later obtain a warrant); however, was rejected by the CRTC as presented.

107. In Order CRTC 2001-279, *Provision of subscribers' telecommunications service provider identification information to law enforcement agencies*, the Commission confirmed that warrantless access to subscriber information, which included even choice of TSP, was not permitted without a tariff and that that tariff should not permit access unless the reason was only to seek a warrant. The Privacy Commissioner of Canada had supported this position and taken the position as well that exceptions to consent under PIPEDA, such as section 7(3)(c.1) of PIPEDA, would not authorize a tariff based on warrantless access. This set a very high bar on release even of telephone number and LSPID information (even the name associated with the number was not released under Bell’s proposed tariff and the Commission’s Order).

108. This very stringent Order[34] was subsequently modified to include three exceptions to the

[33] See CRTC, “Public Notice CRTC 2000-97, Seeking comments on provision of subscribers' telecommunications service provider identification information to law enforcement agencies” (13 July 2000)

[34] The Commission noted that: “19. The Commission considers that the current tariff does not address situations where LEAs, under lawful authority, may require LSPID in circumstances other than an ongoing criminal investigation and when preparing to obtain a warrant. For example, LSPID may be required in order to perform other statutory duties, such as those relating to disasters, security needs, missing persons, etc.”

requirements that the information was being gathered in pursuance of an eventual warrant in a criminal context: national security issues such as terrorism; administration or enforcement of laws or investigations thereof; “preventing imminent harm” (basically, for locating a missing person, or thwarting a crime in progress):

> 22. The Commission therefore finds that the following modified conditions of service are appropriate. To obtain LSPID information pursuant to Bell Canada's tariff, an LEA [law enforcement agency] must identify its lawful authority to obtain the information and indicate that:
>
> i. it has reasonable grounds to suspect that the information relates to national security, the defence of Canada or the conduct of international affairs;
> ii. the disclosure is requested for the purpose of administering or enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or
> iii. it needs the information because of an emergency that threatens the life, health or security of an individual, or the LEA otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.[35]

109. Therefore we find the Commission issuing decisions on “LSPID”, that is, approving a system of “Local Service Provider Identification”, that is, a tariff for law enforcement or other authorities with warrant or subpoena power, to use in making a request to determine which carrier controlled a particular (unlisted) telephone number, and then, subsequently, to which to present a warrant for the additional information information linked to that number (subscriber information, calling records, billing information, etc.).

110. It must be noted, however, above all, that this access provides is the name of the local service provider and not the name of the subscriber associated with it if the phone number is unlisted (and, arguably, not publicly published in the white pages (or online equivalent) public directories) nor any other information, such as calling records, billing information, or address.

111. PIAC acknowledges that these requirements apply to regulated services of telecommunications companies. However, as the Commission has not proceeded to update the confidentiality rules to apply to Internet and mobile wireless services, PIAC submits that effectively the same rules, until such an inquiry is undertaken, should be applied to all TSPs under s. 24 and s. 24.1 as a condition of service.

[35] See: Telecom Decision CRTC (Canadian Radio-television and Telecommunications Commission) 2002-21, Provision of subscribers' telecommunications service provider identification to law enforcement agencies (12 April 2002), which saw the eventual approval of a modified version of Bell’s proposed Tariff Notice 6642.

112. This assertion is supported in relation to IP addresses in particular by the Commission's effective declaration that IP addresses are private information and given the Commission's efforts in Telecom Decision 2006-15 and TRP 2009-657 to ensure customer IP addresses are not used for tracking, identification or individual surveillance and are generally not disclosed without explicit, verifiable consent.

6.2 The Role of Customer Consent in the Disclosure of Customer Confidential Information

113. The Commission has, since the development of the LSPID rules, interpreted the confidentiality of customer information and the privacy policy objective in the *Telecommunications Act* to allow disclosure of CCI in other contexts, only if the TSP has prior, verifiable, explicit consent from customers. Given the nature of the customer's own personal "consent exemption", such consent will permit disclosure of confidential customer information to any non-affiliated third party, provided Commission stipulations are met (and also pursuant to PIPEDA and other general privacy requirements). Therefore, much time and effort has been expended by TSPs, advocates and other interested parties, such as law enforcement, in seeking to define the consent requirements.

114. This the Commission did, definitively, in Telecom Decision 2003-33 (with correction in TD 2003-33-1) and in subsequent modifications made in Telecom Decision 2004-27, and Telecom Decision 2005-15.

115. This latter decision (TD 2005-15) sets out the present acceptable methods for obtaining consent to disclose confidential customer information (at para. 29) under telephony tariffs:

> 29. In light of the above, the Commission directs Canadian carriers to modify their existing tariffs, customer contracts, and other arrangements to amend the list of acceptable methods of obtaining express consent as determined in the last paragraph of Decision 2003-33-1 as follows:
>
> *Express consent may be taken to be given by a customer where the customer provides:*
>
> - *written consent;*
> - *oral confirmation verified by an independent third party;*
> - *electronic confirmation through the use of a toll-free number;*
> - *electronic confirmation via the Internet;*
> - *oral consent, where an audio recording of the consent is retained by the carrier; or*

- *consent through other methods, as long as an objective documented record of customer consent is created by the customer or by an independent third party.*

116. The wording "Express consent may be taken to be given by a customer …" implies an objective standard that the TSP may proceed on an assumption that if they have evidence in the form stipulated, that they may assume that the underlying consent is valid.

117. While this formal indicator may be evidence of, or a defence, for the purposes of, for example, of holding a TSP liable civilly for providing information when the formal CRTC test was met, still, underneath these formal requirements, is the law on the nature of consent. That is, consent still must be obtained validly, especially if the potential for uninformed consent has been communicated to the TSPs.

118. Consent must be free and informed to be valid.[36] Formal requirements that are followed without underlying substantive valid consent do not cure the lack of informed consent.

119. This application, as may be seen from the part on the sign-up processes for COVID Alert and ABTraceTogether, alleges that the prospect of collection and use of IP addresses (and, for ABTraceTogether, telephone number) is not clearly communicated to potential app users and thus vitiates their presumed informed consent, at least in relation to this possibility.

120. We note that the Commission took this approach to requiring clear understanding of the full consequences of information collection, in *Public Interest Advocacy Centre and the Consumers' Association of Canada's applications regarding Bell's use of customer information*, CRTC file #8665-P8-201400762, which, despite being ultimately closed by the CRTC upon receiving notice of agreement with the OPCC in similar complaints, was only done so on condition that Bell implement "express opt-in consent" as per TD 2003-33 and related decision 2005-15.[37]

121. PIAC submits that the COVID Alert sign up process does not constitute valid, explicit consent by the customer under the Commission's present privacy rules for the reasons given above, namely, that nowhere is there a clear description of the potential for TSP subscriber information (or other TSP-held consumer data) to be associated with an IP address used with the

[36] *Englander* v. *Telus Com. Inc.*, (2004) 2004 FCA 387, 328 N.R. 297 (FCA).
[37] See Commission Letter, Subject: Public Interest Advocacy Centre and the Consumers' Association of Canada's applications regarding Bell's use of customer information, CRTC file #8665-P8-201400762 – Requests for Information (17 April 2015); online: https://crtc.gc.ca/eng/archive/2015/lt150417.htm

app.

122. PIAC likewise contends that the consent process in the sign-up for Alberta's ABTraceTogether app does not provide adequate consent for any use of the users IP address, or provided mobile number, for the purpose of seeking additional subscriber information from TSPs, as nowhere in the app sign-up process or elsewhere is the user specifically informed of the possibility of this access to TSP subscriber information by virtue of using the app and associate an IP address with it or by providing a mobile telephone number.

123. PIAC therefore contends that, where, as now, the TSPs are on notice that consent emanating from the apps may be uninformed and not therefore valid, that, despite the formal requirements of TD 2015-15 being met (for example, "*electronic confirmation via the Internet*" from within the apps) that, in relation to the prospect of seeking disclosures related to those data elements (IP addresses or phone numbers) that the TSPs do not in fact already have consent and may not, subject to a new or different consent exemption created by the CRTC, release any customer confidential information or any other related subscriber or personal information.

124. A final consent issue is the existence of previous location or other tracking explicitly consented to by telecommunications users to TSPs in other contexts. For example, several major TSPs run "opt-in" programs of location tracking to offer, for example, discount coupons to consumers using their devices when they enter or approach certain retail locations.[38] In accordance with the law of consent, under PIPEDA and, we submit, the above tariffs, such a "trove" or database of previous location and other data collected under prior consumer consent to location track mobile devices should <u>not</u> be used as previously recorded consent for COVID-19 tracing tools nor permit the use or disclosure of this information without the customer's new, explicit, prior individual. The reason is that this new use, public health, was not part of what customers agreed to in order to enjoy the location-based services offered.

125. Given these positions, we believe that these apps only could collect IP addresses or IP addresses and mobile telephone numbers if they meet the other "public order" exemptions to consent under the Commission's privacy rules under the *Telecommunications Act* or if the CRTC crafts a new public health app exemption.

126. We turn now to consideration of the public order exemptions in the CRTC's rules.

[38] See, for example, Appendix A to our original Application, for Rogers' Privacy Policy which allows such tracking with prior consent.

127. After that, we turn to considering whether the Commission should design a new public health app exemption and specific legal and regulatory test in relation to DCTTs that will maximally protect the privacy of app users.

7.0 PUBLIC ORDER EXCEPTIONS TO CONSENT UNDER PRESENT TELECOMMUNICATIONS PRIVACY LAW

128. As noted above, the process leading to the revised CCI tariffs detailed above, included new exemptions to the customer information confidentiality for telephony of the major incumbent telephone providers. For example, Bell Canada’s General Tariff, No. 6716 (the present terms of service regarding CCI), which still applies to “regulated” services of Bell Canada reads thusly (Item 10: “Terms of Service”, Article 11 “Confidentiality of Customer Records”[39]):

> Article 11: Confidentiality of Customer Records
>
> Note: Continues to apply to local services provided in forborne exchanges
>
> 11.1 Unless a customer provides express consent or disclosure is pursuant to a legal power, all information kept by the Company regarding the customer, other than the customer's name, address and listed telephone number, are confidential and may not be disclosed by the Company to anyone other than:
>
> - the customer;
> - a person who, in the reasonable judgement of the Company, is seeking the information as an agent of the customer;
> - another telephone company, provided the information is required for the efficient and cost effective provision of telephone service and disclosure is made on a confidential basis with the information to be used only for that purpose;
> - a company involved in supplying the customer with telephone or telephone directory related services, provided the information is required for that purpose and disclosure is made on a confidential basis with the information to be used only for that purpose;
> - an agent retained by the Company to evaluate the customer's credit worthiness or

[39] Online: https://www.bce.ca/Tariffs/bellcanada/GT/1/10.pdf?version=1588367123387

to collect the customer's account, provided the information is required for and is to be used only for, that purpose;

- a public authority or agent of a public authority, if in the reasonable judgement of the Company, it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of the information;
- a public authority or agent of a public authority, for emergency public alerting purposes, if a public authority has determined that there is an imminent or unfolding danger that threatens the life, health or security of an individual and that the danger could be avoided or minimized by disclosure of information; or
- an affiliate involved in supplying the customer with telecommunications and/or broadcasting services, provided the information is required for that purpose and disclosure is made on a confidential basis with the information to be used only for that purpose.

(a) Express consent may be taken to be given by a customer where the customer provides:

- written consent;
- oral confirmation by an independent third party;
- electronic confirmation through the use of a toll-free number;
- electronic confirmation via the Internet;
- oral consent, where an audio recording of the consent is retained by the carrier; or
- consent through other methods, as long as an objective documented record of customer consent is created by the customer or by an independent third party.

11.2 The Company's liability for disclosure of information contrary to Article 11.1 is not limited by Article 16.1.

11.3 Upon request, customers are permitted to inspect any of the Company's records regarding their service.

11.4 The Company may also release to a law enforcement agency, in accordance with the terms of a tariff approved by the CRTC, the identity of the service provider, but not the name of the customer, associated with a specific telephone number. [Emphasis added.]

129. PIAC submits that the wording of the above-quoted tariff regarding “imminent danger to life or property” was added by the Commission in responses to Bell Canada’ entreaties to allow it to supply such information to authorities when a situation of an actual crime, such as child exploitation, was occurring in real-time, online, or a missing persons situation, a fire, etc., and not as a blanket permission that could apply to non-urgent, though still potentially, eventually life-

saving matters such as pandemic contact-tracing.

130. PIAC further submits that the wording of the exception "if a public authority has determined that there is an imminent or unfolding danger that threatens the life, health or security of an individual and that the danger could be avoided or minimized by disclosure of information" was intended only for effectively "broadcasting" a warning to all telecommunications users with compatible devices and only "for emergency public alerting purposes" to facilitate public alerting for emergencies such as tornados and active shooters, but not generally for public health tracing or public alerting. It is not worded to apply to specific individuals being traced due to their relation with a confirmed or suspected positive COVID-19 patient nor as a general or blanket request to track or warn all individuals who might be exposed to a positive case.

131. What all of this means is that, PIAC submits, none of the present public order exemptions covers, or can be credibly stretched to cover, an explicit subscriber consent requirement to allow the release of any subscriber information held by a TSP in relation to COVID-app information.

8.0 PUBLIC HEALTH APP EXCEPTION TO EXPLICIT CONSUMER CONSENT TO RELEASE CCI

132. We consider now if the CRTC should design a new public health app explicit consent exception to allow the release of a TSP's subscriber information about a customer upon presentation of information gleaned from a DCTT such as IP addresses or mobile phone numbers associated with COVID Alert or ABTraceTogether (COVID-app information) and specific legal and regulatory test in relation to DCTTs for public health purposes in a pandemic, that will maximally protect the privacy of app users while seeking to effectively reduce infections.

133. Consumers and citizens have several legal, constitutional, ethical and democratically valid reasons for insisting that their TSPs protect their privacy to a high degree: possible reduced civil liberties,[40] the creation of COVID-19 databases and their use in policing and emergency response,[41] and likely discriminatory use (against vulnerable or historically disadvantaged or

[40] See Canadian Civil Liberties Association, "CCLA Live COVID-Liberty Updates" and the links therein, online: https://ccla.org/coronavirus/

[41] See Open Letter of the CCLA, BLAC, HALCO an ALS to Ontario Solicitor General Sylvia Jones, 23 April 2020. Online: https://ccla.org/cclanewsite/wp-content/uploads/2020/04/2020-04-20-Letter-to-Sol-Gen-Final-1.pdf . See also all legal materials in relation to the CCLA et al.'s challenge of O. Reg. 120/20: Order Under Subsection 7.0.2(4) of the Act – Access to Covid-19 Status Information by Specified Persons; online, at: https://ccla.org/health-info-policing/

oppressed groups and individuals) of tracking despite individual consent requirements.[42]

134. To be clear, PIAC believes that the best approach to protecting privacy and balancing it with the social goal of public health would be adequate federal and provincial privacy laws of general application, with an intergovernmental coordination mechanism (joint governments council, MOUs, cross-jurisdictional delegation, etc.) for public interest situations such a public health. We are most dismayed at the federal government's failure to pass privacy laws adequate to control the deployment, distribution and effect of the rollout of the COVID Alert app. This failure, as evidenced by the position of Health Canada that no personal information is implicated in the use of the COVID Alert app, means that the federal app appears to operates in a legal vacuum.

135. Other countries, notably France,[43] have gone to a great extent to seriously and thoroughly consider exposure notification/contact-tracing apps in light of comprehensive public and private sector privacy law, in order to define, limit and control this important and possibly invasive tool.[44] Of course, France has the advantage not only of a specific law governing digitization and use of computers but also the General Data Protection Regulation (GDPR) of the European Union.

136. Québec appears to have realized the utter lack of federal control of COVID Alert in recently announcing it will not support the rollout of COVID Alert in Québec. Note that Québec is presently in the midst of updating its provincial privacy laws, in Bill 64, to be more "GDPR"-like and may be viewing the question of the invasiveness of an app and the seeming inability of present privacy laws as an argument for the more stringent aspects of Bill 64.

137. In this environment, therefore, we believe it all the more important for the CRTC to consider the privacy implications of these apps and the limits placed upon their use, where that use involves telecommunications networks.

[42] See, for example, the concerns outlined by Chris Parsons, senior research associate, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto, "Contact tracing must not compound historical discrimination", Policy Options, 30 April 2020. Online: https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/

[43] See, for example, the Commission Nationale Informatique et Libertés ("CNIL") initial recommendations for implementing "StopCovid" (which is France's non-Google-Apple API-based application); CNIL, April 24, 2020, "Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »"; online : ; courtesy translation [to English] at: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_april_24_2020_delivering_an_opinion_on_a_proposed_mobile_application_called_stopcovid.pdf

[44] See, for example, the Commission Nationale Informatique et Libertés ("CNIL") May 26, 2020 opinion on the conditions for implementing StopCovid ("CNIL Opinion"); CNIL, May 26, 2020, online: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf

138. We also believe that the Commission has consistently upheld a very high standard of customer confidentiality in telecommunications and should continue that tradition for new telecommunications services and for novel situations such as the present epidemic. This means that any proposed disclosure of confidential customer information should meet the existing express consent standards and methods and such consent should not be removed or “implied” or “deemed” automatically by law for pandemic control purposes in general.

139. However, if demonstrably and absolutely needed to effectively implement public health-led contact-tracing, then contact-tracing using confidential customer information generated by TSPs could and possibly should be permitted on a very strict, publicly transparent and time-limited basis and only for those purposes, without express consent of the customer, but with notice.

140. To assist the Commission in possibly developing this regulatory test, for the use of TSPs to evaluate requests for subscriber information related to COVID-app information, strictly by public authorities and to the greater transparency and protection of telecommunications users, and in the absence of a federal statute with guidance as to a public interest override of individual privacy rights in situations such as pandemic control, we outline below what we shall call the “COVID-app disclosure process” or “CADP”. In developing this test, PIAC is inspired by the Aboriginal Legal Services, Black Legal Action Centre, Canadian Civil Liberties Association and HIV & AIDS Legal Clinic Ontario’s (CCLA et al.) pleadings in its litigation to curtail police and other authorities’ indiscriminate access to the personal health information of COVID-19 positive Ontarians who had accessed the Ontario public health system.

141. The litigation of the CCLA’s Application to the Divisional Court to challenge of O. Reg. 120/20: *Order Under Subsection 7.0.2(4) of the Act – Access to Covid-19 Status Information by Specified Persons*, purportedly made under the authority of the *Emergency Management and Civil Protection Act*, RSO 1990, c E9 (“*EMCPA*”), and its exposition and application of legal and constitutional requirements, make excellent starting points for developing a strict test that maximally protects individuals’ privacy while leaving only truly necessary and essential access to subscriber information of TSPs with significant safeguards and transparency requirements.

142. In the CCLA et al.’s Application, the requirement of Ontario’s emergency management orders are described and explained. In short, this regulation-making power is clearly described as extraordinary and time-limited, meant to be as limited as possible to achieve its purpose and to be designed for a specific, constitutional purpose in a free and democratic society and both necessary and likely effective, and not achievable by less intrusive means.

143. The legislation, as described by the CCLA et al.’s Application, requires firstly that the *EMCPA* orders must seek to protect civil rights of citizens - as expressed in that *Act* at subs. 7.0.2(1) - as being subject to the *Charter*. These *Charter* rights are sought to be assured by necessity and essentiality (being limitation to the least intrusive method), as well as effectiveness, requirements, which are found in subss. 7.0.2(2) and (3). Those requirements read:

> **Criteria for emergency orders**
>
> (2) During a declared emergency, the Lieutenant Governor in Council may make orders that the Lieutenant Governor in Council believes are necessary and essential in the circumstances to prevent, reduce or mitigate serious harm to persons or substantial damage to property, if in the opinion of the Lieutenant Governor in Council it is reasonable to believe that,
>
> (a) the harm or damage will be alleviated by an order; and
>
> (b) making an order is a reasonable alternative to other measures that might be taken to address the emergency. 2006, c. 13, s. 1 (4).
>
> **Limitations on emergency order**
>
> (3) Orders made under this section are subject to the following limitations:
>
> 1. The actions authorized by an order shall be exercised in a manner which, consistent with the objectives of the order, limits their intrusiveness.
>
> 2. An order shall only apply to the areas of the Province where it is necessary.
>
> 3. Subject to section 7.0.8, an order shall be effective only for as long as is necessary. 2006, c. 13, s. 1 (4).

144. The CCLA et al.’s Application applies these requirements to the desired disclosure of personal health information (COVID-19 positive status) to public authorities, including police, fire and ambulance personnel (“first responders”).

145. The CCLA et al. contended that such an application to this situation (at para. 19 of their Application) required several practical safeguards to ensure and to publicly and transparently demonstrate that the legislative, exceptional nature of the requirements of the *EMCPA* were met.

146. This list is adaptable to our possible disclosure requests to TSPs for subscriber information

in relation to IP addresses or telephone numbers obtained from COVID Alert, ABTraceTogether or any other DCTT, as the situation is quite similar, with similar imperatives and interests.

147. Re-writing the CCLA et al.’s requirements for TSP subscriber information in the context of telecommunications could be done as suggested below to create a possible regulatory test for subscriber information disclosure. For the “decision” in the CCLA et al.’s Application, we can read in “COVID-app disclosure request” or “CADR”. Thus, a possible proposed test might read:

> A request of a TSP to the CRTC to permit disclosure of a subscriber’s customer confidential information, other subscriber information or any other personal information in the possession of the TSP (“subscriber information” or “customer confidential information”), based on information created by a “COVID app” provided by a Canadian government or public health authority (“COVID-app information”)[45] and proffered as part of a request for related subscriber information, is only valid, and may only be granted, if it meets the following test, referred to as a “COVID-app disclosure request” (“CADR”). Namely:
>
> > (a) the CADR was made reasonably believing that the subscriber information was “necessary and essential in the circumstances” to prevent, reduce or mitigate the spread of the serious illness “COVID-19”;
> > (b) the CADR was made reasonably believing that access to the subscriber information is a reasonable alternative to, or will demonstrably assist in improving, other measures that might be taken to address the illness or spread of the illness, in particular, as an adjunct to manual contact tracing;
> > (c) the CADR was made reasonably believing that the subscriber is the actual user of the COVID-app, and that the COVID-app information relates to the subscriber;
> > (d) the CADR was made on prior notice to the subscriber (or if prior notice were not possible given reasonable efforts, that this notice be provided as soon as possible afterward and in no case later than 48 hours later) and, if notice were given, that efforts to confirm this subscriber’s use has been made, and the subscriber has been given a prior opportunity to dispute that the subscriber is the user of the COVID-app (and an opportunity to make submissions to the CRTC on

[45] By this PIAC means any digital contact tracing technology or “DCTT” as we have defined them, intended to assist controlling the spread of the COVID-19 as caused by the SARS-CoV-2 virus, including, notably, COVID Alert and ABTraceTogether.

these alleged facts if the notice was provided after the CADR was determined by the TSP). Such notice to the subscriber shall sufficiently inform the subscriber of what subscriber information is proposed to be released and upon what COVID-app information the CADR is based;

(e) the affected subscriber has a right to dispute the outcome of such a CADR before the CRTC in a simple process, either before or after the CADR decision. The TSP and any affected public authority may also make representations during such a process, but such representations shall account for the nature of such process, which shall be designed to be open, transparent and simple for the subscriber.

(g) the CADR limits the intrusiveness of the actions authorized by the CADR. Specifically, the CADR sets out the following requirements and limits in relation to actions authorized under the CADR:

(i) by publicly stating, in detail, how, where and how long the COVID-app information that grounded the CADR (typically, the IP address associated with the CADR) can be accessed (that is, whether the IP addresses are located on the federal government’s main key server, a cloud-based server, or both, in what form and with what protections, kept for how long, how accessed and by whom, and how verified or corrected by the subscriber;

(ii) how TSPs and Requester(s) ought to keep track of and publicly report on their CADRs, their outcomes (granted, denied, suspended, withdrawn, etc.), and the number, type and outcomes of dispute processes with subscribers regarding potential access to any subscriber information;

(iii) any limitations on how any provided subscriber information can be used and for what purpose(s) by the public authority or any other private party;

(iv) how the subscriber information ought to be stored by the Requester(s);

(v) how and when the subscriber information ought to be destroyed by the Requester(s); and

(vi) how a complaint about misuse of subscriber information or COVID-app information can be brought.

148. This proposed test is a starting point for permitting access to subscriber information only as strictly necessary, in accordance with maximal privacy protection, and only to actually, effectively, advance contact tracing. We invite commentary by other parties, including TSPs,

governments and health authorities, on how, or even if, there ever would be a justification for access to subscriber information related to COVID-app information in this manner.

149. PIAC submits that the circumstances justifying such disclosure without consent upon the above test would be extremely limited and only for the public interest in public health, in proportion to, and in keeping with, constitutional rights, the avoidance of discrimination against marginalized groups, and the Commission’s long-standing policy of limiting access to subscriber information.

9.0 CONCLUSION AND REQUESTED RELIEF

150. This Application asserts that the COVID Alert app and ABTraceTogether app both associate IP addresses of app users with uploaded positive diagnosis keys and, in relation to the COVID Alert app, with the download of other users positive status keys. These IP addresses are stored in server logs under the effective control of the federal government and Alberta government. With such IP addresses in subscriber logs, such a government can request from a telecommunications service provider (TSP) subscriber information. In addition, the Alberta app asks users to voluntarily provide mobile telephone numbers to use that app. Neither app’s privacy policy, sign-up process nor other documentation, nor public statements, mention the possibility of their government’s ability to request subscriber information based on the users’ IP address or mobile telephone number.

151. This Application asks the Commission to, as a condition of offering telecommunications service (mobile wireless or Internet access) in a privacy promoting manner (under ss. 7, 24, 24.1 and 47) of the *Telecommunications Act*, to:

a) Declare that the confidential customer information rules of the Commission devised for telephony apply to IP addresses and mobile telephone numbers and any other information generated from network connection of digital contact tracing technologies (DCTTs) such as COVID Alert and ABTraceTogether;
b) Prohibit TSPs from disclosing, without explicit consent, any subscriber information requested by any Canadian or foreign government in relation to a DCTT (including COVID Alert and ABTraceTogether) unless such disclosure meets a “COVID-app Disclosure Request (CADR)” as specified by the Commission. Such test must respect the Charter and privacy interests of Canadians and only be applied if such

disclosure is necessary and essential, and cannot be achieved by other means. Such disclosures shall not be used to discriminate against marginalized groups.

152. In addition, the Commission may wish to open a broader inquiry in line with the requests of our initial Application, filed 4 April 2020, which were to:

a) Publicly disclose on the record of this proceeding and to the Commission any steps taken for any government or private interest to facilitate contact tracing;
b) Inquire into any such TSPs’ activities related to contact-tracing apps or network-level facilitation of individual consumer location or other personal or communications details;
c) Require any such TSPs’ activities related to contact tracing respect the confidential customer information rules of the Commission devised for telephony;
d) Prohibit TSPs from using prior consumer consent to location track mobile devices (for example, in “opt-in” marketing programs or other TSP portal or other applications) or to provide databases previously gleaned from these programs to any private or government entities to build, improve or test COVID-19 tracing tools without new, explicit, prior individual consent for this new use or disclosure;
e) Appoint an inquiry officer under subs. 70(1)(a) of the *Telecommunications Act*, to inquire into and report upon contact tracing, as well as to liaise with public health authorities and governments and non-telecom private parties, if necessary;
f) In the alternative, launch a formal Notice of Consultation on the matter.

153. In any case, we believe it is urgent that the Commission consider our primary requested relief, and to propose any disclosure guidelines in the public interest, as the pressure to drive use of DCTTs is likely to increase as Canada faces a potential “second wave” of infections this Fall.

10.0 APPENDIX 1: A “PRIVACY-FIRST” CANADIAN PUBLIC POLICY APPROACH TO DIGITAL CONTACT TRACING TECHNOLOGY (“DCTT”) RELATED TO COVID-19 & FUTURE PANDEMICS

[Please see attached file.]

*** End of Document ***

PUBLIC INTEREST ADVOCACY CENTRE | LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

Position Paper

A "Privacy-First" Canadian Public Policy Approach to Digital Contact Tracing Technology ("DCTT") Related to COVID-19 & Future Pandemics

9 August 2020

TABLE OF CONTENTS

INTRODUCTION & OVERVIEW OF PIAC POSITION PAPER 6

PART 1: COVID-19 PANDEMIC HAS CHANGED THE WORLD & EFFECTIVE CONTACT TRACING IS ESSENTIAL FOR ANY SUCCESSFUL RESPONSE 7

COVID-19 PANDEMIC HAS CHANGED THE WORLD 7
CONTACT TRACING FOR COVID-19 IS A CHRONICALLY MISUNDERSTOOD POLICY ISSUE 8
EFFECTIVE CONTACT TRACING IS ESSENTIAL FOR ANY SUCCESSFUL COVID-19 PANDEMIC RESPONSE 9
Definition Of Contact Tracing 9
Effective Contact Tracing Is Essential 10
Manual & Digital Contact Tracing Are Necessary & Complementary 10
Manual Contact Tracing 10
Digital Contact Tracing 12

PART 2: DIGITAL CONTACT TRACING TECHNOLOGY – WHAT IT IS, HOW IT WORKS & RISKS/BENEFITS 13

DIGITAL CONTACT TRACING TECHNOLOGY ("DCTT"): WHAT IT IS & HOW IT WORKS 13
Digital Contact Tracing Can Be Voluntary Or Mandated 13
Digital Contact Tracing Can Occur At Network Or Application Level 13
Network-Level Contact Tracing 13
Application-Level Contact Tracing 14
CONTACT TRACING APPS ("CTAS"): TYPOLOGY & RISK/BENEFIT ANALYSIS 15
App Typology Is Complex & Based On Purpose, Tracing Technology & Architecture 15
Purpose: Exposure Notification, Risk Awareness & Tracking Apps 15
Exposure Notification Apps 15
Risk Awareness Apps 15
Tracking Apps 15
Tracing Technology: Location-Based & Proximity-Based Apps 16
Geolocation Apps: Monitoring User Contacts Through Location 16
Bluetooth Apps: Monitoring User Contacts Through Proximity 16
Architecture: Centralised & Decentralised Apps 17
Centralised Apps 17
Decentralised Apps 17
Bluetooth Apps (Centralised/Decentralised) Merit Close Attention 18
Centralised v. Decentralised Model 18
Competing Protocols for Each Model 20
Primary Decentralised Protocol: Google/Apple API 21
Apps Have Benefits & Risks (Intrinsic & Extrinsic) 23
Overall Benefits/Risks of Apps 24
Benefits: Potential To Strengthen Public Health Response to COVID-19 Pandemic 24
Risks: Cost, Technology Theatre, Technical, Deliberate Arbitrage, Inequity, Security Breach, Surveillance, Privacy/Civil Liberties Violation & Platform Power 24
Privacy Risks Merit Close Attention 24
App Type-Specific Benefits/Risks 25
Risks Of Exposure Notification, Risk Awareness & Tracking Apps 25
Risks Of Geolocation & Bluetooth Apps 26
Risks Of Centralised & Decentralised Apps 26
Risks Of Bluetooth Apps (Centralised/Decentralised) Merit Close Attention 27
Centralised v. Decentralised Model 27
Competing Decentralised Protocols (Esp. Google/Apple API) 28

PART 3: GLOBAL DCTT – OFFICIALLY DEPLOYED (NETWORK & APPLICATION LEVEL), TEACHING IMPORTANT EARLY LESSONS (ESP. APPS ARE NOT A SILVER BULLET & PRIVACY RISKS ARE REAL & SIGNIFICANT) 30

DCTT (Network & Application Level) Is Officially Deployed *30*
Network-Level Tracing Is Officially Adopted & Deployed In Certain Countries 30
Application-Level Tracing Is Officially Adopted & Deployed Across Regions & Momentum Has Shifted To Decentralised Bluetooth (Esp. Google/Apple API) 31
Official Apps Of All Types Are Deployed Across Regions (National & Sub-National Level) 31
Bluetooth Decentralised (Esp. Google/Apple API) Official Apps Have Global Momentum 32
Google/Apple API Official Apps Differ Between Countries 33
Absence Of Global Coordination Undermines App Effectiveness 33
Global DCTT Deployment, While Still Experimental, Teaches Important Early Lessons *33*
Lesson #1: Overall Risks Of DCTT Are Real & Significant 34
Lesson #2: Public Health Risk – Official Apps Are Not Silver Bullet 34
Deployed Apps Have Low Adoption & Low Impact 34
Voluntary Apps Don't Have Adoption Level Approaching 60% 34
The Most Successful Countries Have No App 35
Deployed Apps' Success Depends On Parallel Manual Tracing & Testing 35
In Countries With High Adoption of Apps & Other DCTT, Physical Restrictions Play Major Role 35
With Or Without DCTT, Re-Emergence From Lockdown Means Increased Infections 36
With Or Without DCTT, A Strong Public Health System is Crucial 36
Lesson #3: Technical Risks – Official Apps Have Technical Problems 36
Lesson #4: Inequity Risks – Official Apps Have Accessibility Problems 37
Lesson #5: Privacy Risks – Official Apps Are Privacy-Invasive 37
Global Privacy-Invading CTAs Must Be Understood In Context Of Broader Geo-Political Trends *39*
Government Responses To Covid-19 Reflect & Reinforce "Techno-Solutionism" 39
Techno-Solutionism Entrenches Big Tech's Power & Push Into Health Sector, Dragging Its Long-Standing Privacy Problem Along For Ride 39
To Win "Global Digital Health Data Race" Governments Support "Medical Big Data Initiatives", With Increasingly Elevated Privacy Problem 42
Global Trend To Sacrifice Privacy For Possibly Ineffective CTAs Poses Danger Of "Orwellian Transformation" To "Big Brother World" 43

PART 4: CANADIAN DCTT – OFFICIALLY DEPLOYED (CTAS) & UNOFFICIALLY DEPLOYED (NETWORK LEVEL) BUT STILL EVOLVING **44**

JURISDICTION OVER COVID-19 PANDEMIC RESPONSE, INCLUDING CONTACT TRACING, IS SHARED BY FPT & MUNICIPAL GOVERNMENTS 44
POLITICAL DEBATE ON DCTT STARTED AFTER INITIAL DEPLOYMENT & FOCUSED ON PROPER OFFICIAL APP LEVEL & TYPE 46
CANADA'S NATIONAL STRATEGY FOR OFFICIAL APPS WAS NOT UNIVERSALLY SUPPORTED BY PT GOVERNMENTS 46
CANADA HAS AN OFFICIAL NATIONAL APP ("COVID ALERT" OR "COVID ALERT CANADA") FOR OPTIONAL ADOPTION & CUSTOMIZATION BY PT GOVERNMENTS 47
GoC Endorsement Of COVID Alert Canada & Ontario Adoption ("COVID Alert Ontario"): 18 June 2020 *47*
Launch Of COVID Alert Canada & COVID Alert Ontario: 31 July 2020 *47*
PT Universal Adoption Of COVID Alert Canada Is Uncertain, Risking Patchwork Approach *50*
Many Official App Options Were Considered By Governments (FPT & Municipal) Before COVID Alert Canada's Endorsement 50
Some PTs Are Still Considering Official App Options 51
CANADIANS' ADOPTION OF COVID ALERT CANADA (OR OTHER OFFICIAL APPS) IS UNCERTAIN 52
Adoption Of COVID Alert Canada: Evolving *52*
Where Canadians Stand On DCTT: Privacy Matters & Stats Show Conflicting Support *52*
Petitions 52
Surveys 53
Media Reports/Interviews 55
IDENTIFYING KEY FEATURES OF OFFICIAL APPS, THEIR INTER-RELATIONSHIP & RELATIONSHIP TO OTHER DATA-DRIVEN GOVERNMENT RESPONSES TO COVID-19 IS ESSENTIAL FOR COMPREHENSIVE PRIVACY ANALYSIS 55
PIAC's Analytical Rubric For Apps Is An Important Tool *55*
COVID ALERT CANADA & ONTARIO: KEY FEATURES 57
COVID Alert Canada *57*

App 58
Data 62
COVID Alert Ontario *65*
App 65
Data 66
COVID ALERT CANADA RELATIONSHIP TO OTHER DATA-DRIVEN FPT GOVERNMENT RESPONSES TO COVID-19 IS TANGLED & UNCERTAIN 66
COVID Alert Canada Relationship To Other DCTT (Official & Unofficial) *66*
COVID Alert Canada Relationship To Broader Digital "Outbreak Response" & Health Technology *67*
GoC & PT Government Engagement In Global Partnership On Artificial Intelligence ("GPAI") 67
PT Governments' Health Data Platforms (Overall) 67
PT Governments' "Enhanced" Manual Contact Tracing Efforts 68
PT PHA Case & Contact Data Management Systems 68
PT Government Recovery Plans Requiring/Recommending Businesses To Provide Data 70

PART 5: CANADA URGENTLY NEEDS "PRIVACY-FIRST" PUBLIC POLICY ON DCTT RELATED TO COVID-19 & FUTURE PANDEMICS, IMPLEMENTED VIA ACCELERATED *PRIVACY LAW REFORM* & INTERIM *PRIVACY RISK-MITIGATION STRATEGIES* ("PIAC RECOMMENDATIONS") 71

PUBLIC POLICY SHOULD SET CONDITIONS FOR RESPONSIBLE DCTT USE IN THE PUBLIC INTEREST, TO MITIGATE DCTT RISKS (ESP. PRIVACY) TO GREATEST EXTENT POSSIBLE 71
Canada's Public Policy Approach To COVID-19 DCTT Was Suboptimal *71*
Sound Public Policy Approach To DCTT Is Vital To Ensure All Risks Of DCTT (Esp. Privacy) Are Mitigated To Greatest Extent Possible *72*
Privacy-Respecting DCTT Is Important Tool To Fight COVID-19 & Future Pandemics *74*
DCTT REIGNITES POLICY DEBATE OVER HOW TO BALANCE PRIVACY & PUBLIC HEALTH-SAFETY: HOW MUCH PRIVACY SHOULD INDIVIDUAL CANADIANS SACRIFICE FOR PUBLIC GOOD IN A PANDEMIC? 75
STRIKE THE *RIGHT* BALANCE WITH "PRIVACY-FIRST" PUBLIC POLICY ON DCTT THAT STRENGTHENS PRIVACY PROTECTIONS, BUILDING ON CURRENT CANADIAN PRIVACY PRINCIPLES & GLOBAL BEST PRACTICE IN PRIVACY POLICY RESPONSES TO COVID-19 76
Global Privacy Policy Responses To COVID-19 DCTT: Carefully Constrained Network-Level Initiatives & Voluntary Bluetooth Decentralised Apps Prioritizing Effectiveness, Necessity & Proportionality *76*
Supranational Government Privacy Policy Responses 76
World Health Organization ("WHO") 76
Organisation for Economic Co-operation And Development ("OECD") 77
European Union ("EU") 77
National Government Privacy Policy Responses 80
United States 80
France 81
United Kingdom 81
Australia 81
Switzerland 82
Overall 82
Experts' Recommendations on Privacy Policy Responses 82
Global Experts 82
Canadian Experts 84
IMPLEMENT PRIVACY-FIRST POLICY ON DCTT VIA ACCELERATED CANADIAN PRIVACY LAW REFORM 85
Canadian Privacy Law Is Complex & Further Complicated By COVID-19 *85*
"Privacy" Means Privacy of "Personal Information", Broadly Defined 85
Legal Framework For Protecting Personal Information ("Privacy Law") Governs Its Collection, Use & Disclosure 87
Privacy Law Is Quasi-Constitutional & Recognizes Need To Balance Other Interests (e.g., Public Health-Safety) 87
Privacy Law Has Myriad Sources & Competent Authorities 87
Privacy Statutes & Privacy Commissioners 87
Sector-Specific Statutes With Privacy Provisions: Telecommunications Act & CRTC 89
Privacy Torts, Other Protections & Courts 90
Exceptions To Privacy Protections For Emergency Or Public Health Crisis ("Privacy Exceptions") 90
Privacy Protections/Exceptions Further Complicated By Siloed Approach To Canadian Public Health Policy 92

Heart Of Privacy Law Is Privacy Protections 93
Privacy Principles 94
Individual Rights 95
Key Privacy Issues: Privacy Impact Assessment ("PIA"), Employee Monitoring & International Data Transfer 96
Conclusion: DCTT Is Subject To Myriad, Complex, Overlapping, & Inconsistent Canadian Privacy Laws 97
COVID-19 Highlights Gaps In Canadian Privacy Protections Pertaining To Digital Technologies ("Digital Privacy Gap"), Accelerating Need For Privacy Law Reform 97
There Is A Digital Privacy Gap, Driving Need For Statutory Reform 98
There Is A Digital Privacy Gap 98
Bridging Digital Privacy Gap Requires Modernizing & Strengthening Privacy Legislation 98
Interim Privacy Commissioner Response To Digital Privacy Gap Is Guidance On Digital Technology 100
Digital Privacy Gap Is Highlighted By COVID-19 (Esp. DCTT), Accelerating Need For Statutory Reform 100
COVID-19 (Esp. DCTT) Highlights Digital Privacy Gap 100
Interim Privacy Commissioner Response To Pandemic-Highlighted Gap Is Guidance On COVID-19 (Incl. DCTT) 101
Urgent Need For Statutory Reform Is Reinforced By: Privacy Commissioners' Assessment Of COVID Alert Canada, PT Privacy Law Overhauls & Court Decisions On Privacy (Domestic & Global) 101
PENDING BROADER PRIVACY LAW REFORM, IMPLEMENT PRIVACY-FIRST POLICY ON DCTT VIA RISK-MITIGATION STRATEGIES FOR CANADIAN GOVERNMENTS, REGULATORS & OWNER/OPERATORS OF DCTT (PUBLIC, PRIVATE & PUBLIC-PRIVATE) 103
Government (FPT) Privacy Risk-Mitigation Strategies for DCTT 103
Regulator (FPT) Privacy Risk-Mitigation Strategies for DCTT 104
Privacy Commissioner (FPT) Risk-Mitigation Strategies For DCTT 104
CRTC Privacy Risk-Mitigation Strategies For DCTT 105
DCTT Owner/Operators (Public, Private & Public-Private) Privacy Risk-Mitigation Strategies 106

CONCLUSION 106

APPENDIX A: COVID ALERT CANADA SCREENSHOTS 107

COVID Alert Canada Introduction Screens 107
Learning About How COVID Alert Works 108
Turning On Exposure Notifications 109
Entering The One-Time Key 110
The Privacy Policy 111
Exposure Notification Settings In Android Settings 113
Positive Exposure Notification Screens (Publicly Available Images) 115

APPENDIX B: FEDERAL PRIVACY PRINCIPLES – PRIVACY ACT, PIPEDA & OPCC GUIDANCE 116

PRIVACY PRINCIPLES UNDER PRIVACY ACT 116
PRIVACY PRINCIPLES UNDER PIPEDA 117
PRIVACY PRINCIPLES UNDER OPCC GUIDANCE (PRIVACY ACT & PIPEDA) 118
General Guidance (Key Only) 118
OPCC Guidance On Mobile Apps 118
OPCC-Alberta & BC Guidance On Meaningful Consent (Incl. Location Data) 120
OPCC Guidance On Data Breaches 120
COVID-19 Guidance 121
May 2020 Joint OPCC-PT Privacy Commissioner Guidance To FPT Governments On DCTT 121
April 2020 OPCC Guidance To GoC 122
March 2020 OPCC Guidance To GoC & Businesses 124

APPENDIX C: BIBLIOGRAPHY 126

ENDNOTES* 156

INTRODUCTION & OVERVIEW OF PIAC POSITION PAPER

1. **PIAC.** The Public Interest Advocacy Centre ("PIAC") is a national not-for-profit organization and registered charity that represents the interests of consumers, and in particular, vulnerable consumers, in important public services. PIAC has been actively engaged in privacy issues since the early 1990s, with representatives sitting on the Canadian Standards Council Committee that led to the introduction of PIPEDA, filing complaints with the Office of the Privacy Commissioner of Canada ("OPC", "OPCC", "Canadian Privacy Commissioner", or "Privacy Commissioner of Canada") on privacy standards in consumer transactions throughout the early 2000s, and publishing several reports on PIPEDA and consumers. Most recently, Most recently, PIAC filed a Part 1 Application with the Canadian Radio-television and Telecommunications Commission ("CRTC"), on 4 April 2020, requesting CRTC guidance on the role of telecommunications service providers (TSPs) in contact-tracing apps. On 17 August 2020, the CRTC finally responded to PIAC's initial application in a Letter Decision. The Commission found that the public interest was not best served by appointment of an Inquiry Officer or the issuance of a Notice of Consultation at that time. The present document is now an Appendix to a new Application by PIAC, dated today.

2. **Purpose.** "Contact tracing is one of the most discussed and misunderstood policy issues as we grapple with COVID-19".[1] The purpose of this PIAC position paper is threefold:

   - to shine a light on rapidly evolving COVID-19 digital contact tracing technology ("DCTT"[2]), including contact tracing application ("CTA"), developments in Canada and their significant privacy implications for Canadians, ideally before their mass deployment;
   - to provide a conceptual framework and taxonomy for digital contact tracing that can be used by federal and provincial/territorial ("FPT") privacy commissioners and the Canadian Radio-television and Telecommunications Commission ("CRTC") to ground their respective analyses of DCTT in context of COVID-19 and future pandemics; and
   - to help inform the broader privacy debate, especially the ongoing Government of Canada ("GoC") review of federal privacy legislation and Ontario government consultation to "improve the province's privacy protection laws"[3].

3. **Parts.** The PIAC position paper, which is current to August 15, 2020 (unless otherwise noted), has five parts:

   - Part 1: Contends the COVID-19 pandemic has changed the world and effective contact tracing, both manual and digital, is needed for any successful response.
   - Part 2: Provides a conceptual framework and taxonomy for DCTT.
   - Part 3: For context, describes the current state of global DCTT.
   - Part 4: Describes the current state of Canadian DCTT, focused on Canada's official national CTA "COVID Alert".
   - Part 5: Recommends a **"privacy-first" Canadian public policy on DCTT related to COVID-19 and future pandemics, implemented via accelerated privacy law reform and interim privacy risk-mitigation strategies by governments, regulators, and DCTT owner/operators**. This includes a high level overview of current Canadian privacy law pertaining to DCTT, which is extremely complex, including the *Personal Information Protection and Electronic Documents Act*[4] ("PIPEDA"), the *Privacy Act*[5] ("Privacy Act"), and OPCC and provincial/territorial ("PT") privacy commissioner guidance on privacy and COVID-19.

4. For clarity, this position paper does not conduct a PIAC privacy assessment of COVID Alert or take any position on the adequacy of FPT privacy commissioners' privacy assessments thereof. For this assessment, please see PIAC's separate Part 1 Application to CRTC dated 9 September 2020. In this Application, **we are not trying to discourage Canadians from using the COVID Alert app, rather to highlight potential access to telecommunications subscriber information via IP address use and that should be addressed by the CRTC to further protect Canadian's privacy, especially as adoption of the app grows.**

5. In particular, we believe the **public health benefits of COVID Alert, *in its current form*, outweigh its privacy risks sufficiently for us to recommend adopting the app** (ideally with virtual private network "VPN" use until the CRTC rules on our Application) for the purpose of stopping or slowing the spread of the virus as part of a broader public policy response to the COVID-19 pandemic. Indeed, we applaud GoC for adopting and launching an *almost privacy-first* CTA that could be a model for other democratic countries to follow. However, we also recommend that **certain measures should be taken to further protect Canadians' privacy**:

   - CRTC: should, on an urgent basis, address remaining privacy issues with COVID Alert, specifically the potential leakage of IP addresses (which may on their own constitute "personal information" and with which, upon presentation to TSPs, may provide the key to obtaining subscriber information);
   - GoC: should, on an urgent basis, address accessibility and broader social equity issues with COVID Alert (including issues that arise from, or are exacerbated by, Canada's "digital divide");
   - FPT privacy commissioners: should collaborate with CRTC to prevent IP address leakage at the TSP (network) level, and independently vet any changes to COVID Alert's functionality or data flows before they are implemented and ensure these are notified to users in a way that ensures meaningful and informed consent; and
   - FPT governments and privacy commissioners: should engage in continuous, transparent monitoring and evaluation of COVID Alert's effectiveness, privacy protections, and third-party components (e.g., Google/Apple API) and ensure the app is decommissioned and all its associated data deleted when the pandemic is deemed to be over or the app is deemed to be ineffective, whichever is earlier.

6. **"Privacy".** Since privacy has many meanings, it is important to transparently define its intended usage in this document: "privacy" means privacy of "personal information", broadly defined (see details in Part 5).

PART 1: COVID-19 PANDEMIC HAS CHANGED THE WORLD & EFFECTIVE CONTACT TRACING IS ESSENTIAL FOR ANY SUCCESSFUL RESPONSE

7. The COVID-19 pandemic has changed the world and effective contact tracing is essential for any successful response.

COVID-19 PANDEMIC HAS CHANGED THE WORLD

8. With high transmissibility, a case fatality rate greater than 1%, and no effective antiviral vaccine or therapy, COVID-19 is a global pandemic[6] that has changed the world:

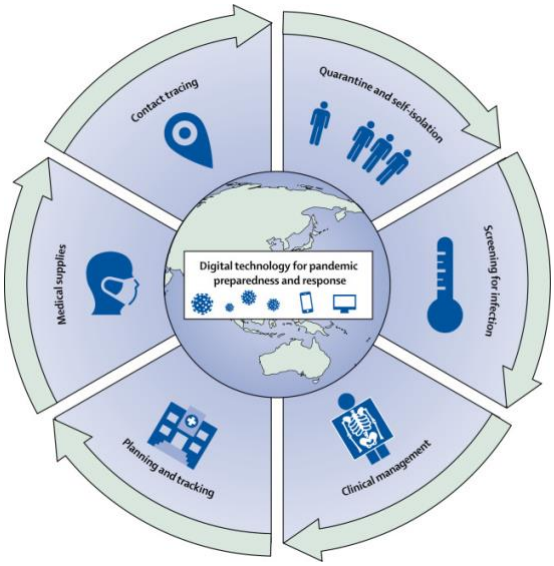
> *"The SARS-CoV-2 (Covid-19) outbreak is the most widespread pandemic in a century and is currently the largest global crisis since the Second World War. The pandemic has created a global health emergency that has drastically impacted all aspects of modern life and has strained global healthcare systems, economies, and political institutions. Our rapidly evolving understanding of Covid-19 has challenged evidence-based decisions regarding strategies used to contain and prevent the spread of the virus."*[7]

> *"With over 100 countries having gone into lockdown, the COVID-19 pandemic triggered the third and greatest economic, financial and social shock of the 21st century, after 9/11 and the global financial crisis of 2008. This systemic shock triggered a halt in global production, hitting supply chains across the world, a steep drop in consumption together with a collapse in confidence and, finally, a sharp decline in services that reflects the consequences of lockdowns and social distancing, especially in urban settings. The OECD estimates that GDP in OECD countries will contract by 9.5% in 2020 if there is a second wave of Covid-19 infections."*[8]

9. On August 10, 2020, global confirmed coronavirus cases surpassed 20 million (including 730,000 deaths) and Canada's cases passed 120,000 (including 9,000 deaths).[9] However, COVID-19 is still a new disease

"about which we still know quite little (…) In some, it can be fatal or cause permanent harms, including serious lung damage or limb amputations. In others, it can cause no or minimal symptoms. Asymptomatic or pre-symptomatic individuals can still infect others. It may be possible for one individual who has already had the illness to become sick again."[10]

10. "Government-coordinated efforts across the globe have focused on containing and mitigation, with varying degrees of success"[11], using strategies that include surveillance, testing, contact tracing, quarantine/self-isolation, and health care/clinical management[12] ("COVID-19 pandemic strategy"). The COVID-19 pandemic strategy can be, and is, facilitated by digital technology ("digital health technology")[13] (see infographic below[14]). Many countries remain in pandemic "lockdown", defined as "situations where people are ordered to stay home, except for essential trips and people aren't allowed to mingle with anyone outside of their own household"[15] ("stay-at-home-orders"), or at least with social/physical distancing measures.



11. The rest of this document focuses on one element of the COVID-19 pandemic strategy: COVID-19 contact tracing.

CONTACT TRACING FOR COVID-19 IS A CHRONICALLY MISUNDERSTOOD POLICY ISSUE

12. A June 2020 report by Ryerson University's Cybersecure Policy Exchange ("CPE") correctly asserts that **"(c)ontact tracing is one of the most discussed and misunderstood policy issues as we grapple with COVID-19"**.[16]

13. For this reason, PIAC believes that contact tracing merits a deep-dive, especially from our unique consumer-citizen perspective. Consumer research inputs for public policy decision-making on contact tracing in the context of COVID-19 and future pandemics are vital to ensure the interests of Canadians as consumer-citizens are considered and optimized by all levels of government (i.e., federal, PT, and municipal). Consequently, this policy-oriented paper takes a comprehensive and evidence-based approach that:

- explains why contact tracing matters, what it is, and how it works;
- explores the current state of *digital* contact tracing around the world and the lessons it teaches;
- describes the current state of Canadian digital contact tracing; and
- recommends a "privacy-first" Canadian policy response to digital contact tracing, informed by best practices in public policies regarding privacy and digital contact tracing in democratic countries. For

clarity, PIAC does not use this privacy-first approach to *evaluate* existing Canadian digital contact tracing initiatives. For this evaluation, please see our Part 1 Application to the CRTC.

EFFECTIVE CONTACT TRACING IS ESSENTIAL FOR ANY SUCCESSFUL COVID-19 PANDEMIC RESPONSE

14. *Effective* COVID-19 contact tracing is an essential element of any potential successful public health response to the pandemic.[17] In the words of the World Health Organization ("WHO"), "(c)ontact tracing is an essential public health measure and a critical component of comprehensive strategies to control the spread of COVID-19".[18]

DEFINITION OF CONTACT TRACING

15. **Definition.** Contact tracing is a process used to *identify, notify, educate, and monitor* individuals who have contact with an infected person[19] and it is "a well-understood tool to tackle epidemics"[20]. According to WHO:

> *"Contact tracing breaks the chains of human-to-human transmission by identifying people exposed to confirmed cases, quarantining them, following up with them to ensure rapid isolation, and testing and treatment in case they develop symptoms. When implemented systematically and effectively, these actions can ensure that the number of new cases generated by each confirmed case is maintained below one."*[21]

16. **Purpose(s).** In the context of COVID-19, the primary purpose of contact tracing is to help with infection control[22] (i.e., to "contain the spread of the virus"[23]), because individuals in contact (especially close) with an infected person have a higher risk of becoming infected and sharing the virus with others[24]. It is estimated that each infected person can, on average, transmit the virus to two or three others, and that one infected person can, in 10 rounds of transmission, result in more than 59,000 cases.[25]

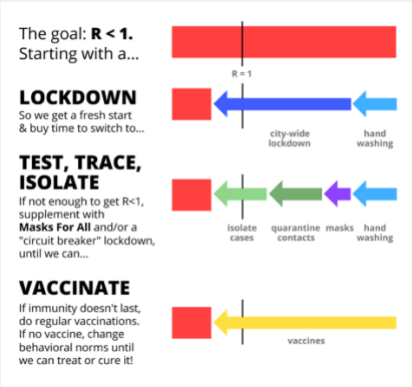
> *"The spread of infection can be prevented by tracing the route of transmission, especially for close contacts. The important thing is to minimize the spread of infection in the country by preventing one cluster of patients from creating another cluster."*[26]
>
> *According to WHO: "contact tracing requires identifying persons who may have been exposed to a person with COVID-19 and following them up daily for 14 days from the last point of exposure. Since COVID-19 transmission can occur before symptoms develop, contacts should remain in self-quarantine during the 14-day monitoring period to limit the possibility of exposing other people to infection should they become ill".*[27]

17. Contact tracing can also be used for secondary purposes, including to monitor and enforce compliance with government guidelines and rules about COVID-19 (e.g., shielding, social/physical distancing, or quarantine)[28] and providing public health authorities ("PHAs") with epidemiological insights into the virus so they can better manage it[29]. For present purposes, "public health authorities" and "public health officials" refers to individuals employed by government entities (e.g., municipal/local, PT, and federal health departments, ministries, and agencies) who attained their position based on professional merit ("public health professionals", e.g., doctors and nurses), political appointment (e.g., FPT chief public health officers), or political election (i.e., the elected executive, e.g., ministers of health).

18. **Prospective and retrospective.** Contact tracing can be done prospectively, tracing contacts of the infected person as potential future cases to be tested and perhaps quarantined ("prospective contact tracing") and retrospectively, tracing backwards from the infected person to document the chain of transmission and identify a common source for clusters of multiple cases ("retrospective contact tracing").[30] Retrospective tracing is important because "(o)ften it's not the person who tested positive for the coronavirus that is spreading the disease, it's the person that gave it to them – a sort of super-spreader or 'Patient Zero'".[31]

EFFECTIVE CONTACT TRACING IS ESSENTIAL

19. Contact tracing only works in certain circumstances, including: participation from the population being traced (mandated or voluntary); and together with other public health measures ("PHMs"), especially "in concert with 'robust testing capacity,' and somewhere for sick people to quarantine. The path to glory is 'Test, trace, isolate'"[32] (see infographic[33]):



MANUAL & DIGITAL CONTACT TRACING ARE NECESSARY & COMPLEMENTARY

20. *Manual and digital* contact tracing is important and necessary to safely manage the relaxation of COVID-19 pandemic lockdown (aka "reopening the economy" or "deconfinement").[34]

MANUAL CONTACT TRACING

21. Historically, contact tracing was only performed manually ("manual or analog contact tracing"), by PHAs, based on interviews and phone calls with diagnosed infected people to assemble an interaction graph. Manual contact tracing remains "the primary strategy" used by global PHAs to reduce COVID-19's spread[35] (see infographic[36]) and, if done "perfectly", it can stop propagation of the virus.[37]

22. **Manual contact tracing infrastructure.** According to WHO, effective (never mind perfect) manual contact tracing requires "manual contact tracing infrastructure" that – in addition to public participation and PHMs – includes: "careful planning and consideration of local contexts, communities, and cultures; a workforce of trained contact tracers and supervisors; logistics support to contact tracing teams; and well-designed information systems to collect, manage, and analyse data in real-time."[38]

23. **Contact tracers.** A sufficient number of contact tracers and their ability to gather information from infected individuals is a key factor. The number of contact tracers that is sufficient for successful tracing is country-specific. For example, on June 23, 2020, the Director of the US Centers for Disease Control and Prevention told Congress that successful tracing would require a total of 100,000 contact tracers (as of June 17, the US had approximately 37,000) and the US public health standard for each state is 30 contact tracers per 100,000 residents (as of June 25, met by only seven states).[39]

24. Even with the proper number of contact tracers, their ability to gather information depends on factors including the degree of "trust" in the system, which depends on factors such as reliability, ideology, and privacy, since, even in its manual form, "(c)ontact tracing is a very intrusive program"[40]. Again, the US is illustrative. In New York City, an early pandemic epicenter, contact tracers struggled to locate infected people and only half of confirmed infected people provided information. It is feared that the administration's failure to specify how privacy will be protected could limit the reach of tracers' efforts, in large part because the City's experience demonstrates that "(d)ata is so seductive" since "(o)nce you have these data sets, there's so many reasons to use them"[41] and, in particular, the City has a mixed record with privacy in certain communities (e.g., treatment of immigrants, Arabs, and Muslims) that makes peoples "very nervous that every little bit of information will be used against them"[42]:

"'Community members must have confidence that the information that they provide to contact tracers is truly confidential,' Bethsy Morales-Reid, senior director for health initiatives for the Hispanic Federation, said at a recent Council hearing. 'When you ask a Covid-19-positive person who they have come in contact with, you're asking them to give up their undocumented tía [aunt] who helps them raise their children or their elderly mother who lives with them and may not be listed in their lease agreement.'"[43]

"Muslim New Yorkers have not forgotten the massive surveillance operation perpetrated by the NYPD in the years following Sept. 11. The Associated Press revealed in 2011 that police spied on heavily Muslim neighborhoods, used informants and monitored residents who had not been accused of a crime or suspected of criminal activity. [new para] 'I don't expect [the city] to get answers from the Arab and Muslim community because of the past surveillance that's been done,' said Yafa Dias of the Arab American Association of New York. 'They've felt so much hate and mistrust, and it still makes them anxious.'"[44]

In Texas, about 1,500 co-plaintiffs, including current and former state representatives, filed a lawsuit against the Governor over the state's $295M program, on grounds it violates the First, Fourth and Fourteenth Amendments[45] and Massachusetts drastically scaled back its program after complaints from local PHAs that it was unreliable.

25. **Inherent limitations.** Manual contact tracing has inherent limitations, such as inability to detect infected individuals who are pre-symptomatic (which is when COVID-19 appears to be most contagious) or asymptomatic, and time delays.[46] Hours, never mind days, matter, as one doctor explains: "This particular patient may have spread COVID to multiple people who are going to come to my ICU a week from now. The longer it takes to start contact tracing, the more complex that task is for the contact tracers because more time has passed."[47] Further, while manual tracing can be very effective at the early stages of a potential epidemic, the efficacy of manual tracing declines afterwards, as the number of infections increases and requires corresponding growth in the number of contact tracers.[48] These concerns are exacerbated by the possibility of a "second wave" of COVID-19, which medical experts say is "inevitable" and could be worse than the first.[49]

DIGITAL CONTACT TRACING

26. **Digital contact tracing technology ("DCTT").** Today, contact tracing can also be conducted automatically ("automatic contact tracing")[50], using digital technology ("digital contact tracing technology [DCTT]" or "digital contact tracing"). Digital contact tracing for COVID-19 "is new and no-one's done it at scale before (…) (s)o we're all learning simultaneously across the disciplines of epidemiology, socio-technical interaction, engineering, modelling and privacy and security".[51] However, it is generally agreed that digital contact tracing is not a silver bullet[52] or panacea, but rather complements manual contact tracing, by increasing PHAs' capacity to respond quickly to new infections[53] and to empower manual tracers to make informed decisions.[54] As noted, digital contact tracing is especially important for COVID-19, because manual contact tracing alone is "too slow for COVID-19's ~48 hour window".[55]

27. **Broader digital "outbreak response" technology**. DCTT can be used alone or together with broader "outbreak response tools", defined by WHO as digital technologies that are designed for PHAs to "manage dynamic relationships between cases and contacts" through "electronic data entry of case and contact information" into "relational databases" that "can be used to facilitate all aspects of contact tracing, including case investigation, listing and monitoring of contacts, and automating analysis and performance monitoring".[56] Outbreak response technology, in turn, can be linked to the broader public health system via digital "health" technology[57], which can be linked to non-health sectors via "data-driven" technology (i.e., information technology ["IT"]), which is inherently "privacy impactful" technology[58].

PART 2: DIGITAL CONTACT TRACING TECHNOLOGY – WHAT IT IS, HOW IT WORKS & RISKS/BENEFITS

28. Knowing what digital contact tracing is and how it works, and identifying its risks and benefits (intrinsic and extrinsic), is the necessary foundation to determine and analyze its real-world implementation and impacts.

DIGITAL CONTACT TRACING TECHNOLOGY ("DCTT"): WHAT IT IS & HOW IT WORKS

29. Digital contact tracing technology is complex and multi-faceted.

DIGITAL CONTACT TRACING CAN BE VOLUNTARY OR MANDATED

30. Digital contact tracing can be voluntary or required by the government ("mandated").

DIGITAL CONTACT TRACING CAN OCCUR AT NETWORK OR APPLICATION LEVEL

31. Digital contact tracing can take place at the network level ("network-level contact tracing") or application level ("application-level contact tracing", "app-based contact tracing", or "contact tracing apps [CTAs]").

NETWORK-LEVEL CONTACT TRACING

32. **Network-level contact tracing (TSPs).** Network-level contact tracing involves data transmitted over telecommunications networks ("telecommunications data" or "network data") by telecommunications service providers ("TSPs"), including Internet access service providers ("ISPs") and wireless access service providers ("WSPs") such as mobile/cellular phone companies ("cellphone companies"). TSPs, as part of their normal course of business, *collect, retain, and process/analyze* subscriber data, including "location data", defined as information about the geographic position of a mobile device at a particular time. This data can be used internally or externally (i.e., shared with third parties, either TSPs or non-TSPs), in exchange for a monetary fee ("commercial exploitation") or without charge ("free").

33. **Other collectors of location data (technology companies/information society service providers).** Technology companies (e.g., Google and Facebook) also collect location data, via applications whose functionality requires its use, and it is "significantly more precise" than TSPs'.[59] Google, which produced the Android mobile operating system (the world's most popular) and operates navigation apps Google Maps and Waze, "has a particularly extensive trove of data".[60] Other companies that collect location data include owners of e-commerce apps, however it is "regarded by technology experts as less comprehensive and reliable than data from other sources".[61]

34. **Location data use in COVID-19 pandemic strategy.** According to the European Data Protection Board ("EDPB"), location data can help to model the spread of COVID-19 and the overall effectiveness of confinement measures[62] and, when used for this purpose, has "two principal sources": "location data collected by *electronic communication service providers* (such as mobile telecommunications operators) in the course of the provision of their service; and location data collected by *information society service providers'* applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.)"[63]. For this reason, the rest of this document uses "location data" to mean location data originating from TSPs and/or information society services. Where there is a need to disintermediate these types of location data due to jurisdictional or other concerns, we make that use explicit.

APPLICATION-LEVEL CONTACT TRACING

35. **Application-level contact tracing.** Application-level contact tracing involves software deployed on a mobile device (e.g., smartphone or wearable[64]) that is specifically designed to carry out contact-matching to identify people potentially exposed to COVID-19 and alert them they could be infected, pose a risk of contagion, and need to self-isolate to prevent further spread. App-based contact tracing is appealing because it is fast:

> *"App-based contact tracing is appealing in part because the coronavirus' spread is so stealthy. Infected people can transmit the virus for days before they develop symptoms, and it can take several more days for public health investigators to learn about a case and confirm it with testing. These teams then have precious little time for traditional contact tracing: interviewing the infected person, tracking down all the recent contacts they can recall, and getting those people to self-isolate before they, too, pass on the virus.*
>
> *Local health departments, many of them understaffed, are straining to keep up. 'By the time you get the data, you have a couple days to chase people down,' says C. Jason Wang, a health policy researcher at Stanford University who is working with health departments on their COVID-19 response. But if smartphones could detect when two users are close enough to share the virus, an app could alert one person as soon as the other gets sick—even if those people are strangers who just happened to sit in adjacent subway seats. 'The technology response is absolutely necessary,' Wang says, 'and it needs to be fast.'"*[65]

36. **Development, adoption, and deployment of CTAs.** Contact tracing apps can be built/developed from scratch[66] or adapted from existing apps[67] (whose source code is either proprietary ["proprietary apps"] or open ["open source apps"]) and adopted/sanctioned/endorsed and deployed by governments (specifically, PHAs) ("official apps" or "sanctioned apps"[68]) or non-government entities ("unofficial apps" or "third-party apps"[69]). Official apps can be owned by the government or owned by business and operated in partnership with government ("public-private sector partnership").

37. **Effective CTAs.** Contact tracing apps can only be effective – however "success" is defined (e.g., slowed rate of infection and changed course of pandemic) – if they are adopted and, as noted, accompanied by a strong public health system with *sufficient testing* to enable infected individuals to accurately self-report and capacity to connect them with social supports to help them self-isolate.[70] Experts emphasize that testing, tracing, and self-isolating are issues requiring difficult political decisions specific to each country, therefore "(t)here's not going to be a single app's back end that you can take from one country and just plop it down in another country".[71] Adoption of CTAs warrants further attention.

38. **Adoption of CTAs**. The primary condition for success is that apps are widely adopted (i.e., downloaded, installed, and used). According to a study by epidemiologists from Oxford University[72] ("Oxford Study") – which was initially misreported – the required penetration level to "suppress the pandemic on its own, without any other form of intervention" is "80% of all smartphone users", which "excludes groups less likely to have a smartphone and is equivalent to 56% of the overall population". However, apps "star(t) to have a protective effect" at "much lower levels", meaning that "other prevention and containment measures will be required", such as "social distancing, widespread testing, manual contact tracing, medical treatment, and regional shutdowns", and "ha(ve) an effect at all levels of uptake" (e.g., "one infection will be averted for every one to two users).

39. Wide adoption can be achieved by the government mandating adoption ("mandated apps") or, if adoption is voluntary[73] ("voluntary apps"), if apps are "trusted"[74] sufficiently for significant take-up and there is equal access to mobile devices, particularly to smartphones, especially current models[75]. Trust in CTAs requires transparency, security and privacy protections, and government endorsement (ideally at the national level).

40. **CTAs (mandated or voluntary) can be required by public or private sector entities to access spaces, services, or benefits.** It is important to note that whether or not contact tracing apps are mandated by the government, they can be *required by public sector entities in order to access public spaces or government*

services/benefits and/or by private sector entities (e.g., employers, physical businesses, and institutions). In particular, employers can require CTAs to protect the health and safety of their workplaces, pursuant to employment law occupational health and safety ("OHS") requirements (see details below).[76]

CONTACT TRACING APPS ("CTAS"): TYPOLOGY & RISK/BENEFIT ANALYSIS

41. This section identifies key types of contact tracing apps and their inherent benefits/risks (aka "pros/cons"). The discussion is high-level only and intended to provide a conceptual foundation for the factual, policy, and legal discussion that follows.

APP TYPOLOGY IS COMPLEX & BASED ON PURPOSE, TRACING TECHNOLOGY & ARCHITECTURE

42. There is a complex typology of contact tracing apps, distinguished on the basis of key factors including purpose, tracing technology, and architecture.

PURPOSE: EXPOSURE NOTIFICATION, RISK AWARENESS & TRACKING APPS

43. Based on their purpose (aka "use" or "functionality"), contact tracing apps are distinguished into exposure notification, risk awareness, and tracking apps, which can be deployed alone or together (as complements). Further, each of these app uses can be accompanied by additional functionalities that "assist its users in making actionable decisions and (…) in the development of better epidemiological models and better public (health) policies"[77], such as: PHA contact facilitation; information provision; symptom checker; telehealth; quarantine administration/enforcement; immunity passport (aka "immunity certificate" or "health passport"); and aggregated data analytics.[78]

EXPOSURE NOTIFICATION APPS

44. Exposure notification apps "detect *contact* with other such devices to indicate its owner has been sufficiently close to facilitate the potential transmission of a COVID-19 infection"[79] and, when users test positive for COVID-19, they instruct the app to send a warning ("exposure notification") direct to those with a similar app whose mobile ID has been connected.[80] These apps *prima facie* do not send mobile IDs gathered by the app *to PHAs* for decryption and follow-up with individuals.[81]

RISK AWARENESS APPS

45. Risk awareness apps are an enhanced version of exposure notification apps that identify "*risky* contact", because "(t)he risk of 'contact' with someone who later becomes symptomatic is very different, depending on whether you walked past them on the street, or had a cosy dinner with them".[82] These apps use artificial intelligence ("AI"), specifically a "machine-learning (ML) algorithm", to process "clues" (e.g., prior medical conditions, age, biological sex, risk levels of all contacts, and when these contacts happened) and calculate a "risk factor" (i.e., predict probability) for infection, thereby providing "early warning signals, well before standard tracing (digital or manual) would raise (a) flag".[83]

TRACKING APPS

46. Tracking apps track the *location* of infected individuals – via the use of geolocation data[84] (see details above and below) – to help PHAs know where they are/were, for example, isolated or in public, infecting others.

TRACING TECHNOLOGY: LOCATION-BASED & PROXIMITY-BASED APPS

47. Based on their tracing technology, which logs contacts between two users, apps are distinguished into location-tracking ("location-based apps" or "geolocation apps") and proximity-detecting ("proximity-based apps" or "Bluetooth apps")[85], which respectively use geolocation and Bluetooth data present in smartphones.

48. A single app can be *both* location- and proximity-based (e.g., GPS location is given for a proximity event).[86]

GEOLOCATION APPS: MONITORING USER CONTACTS THROUGH LOCATION

49. To log contacts between two users, geolocation apps use geolocation (e.g., Global Positioning System ["GPS"], cell tower triangulation, WIFI fingerprinting, or mobile device ID[87]). In particular, they "identify a person's contacts by tracking the phone's movements and looking for other phones that have spent time in the same location".[88] Geolocation data is *necessarily* sent to a centralized location.[89]

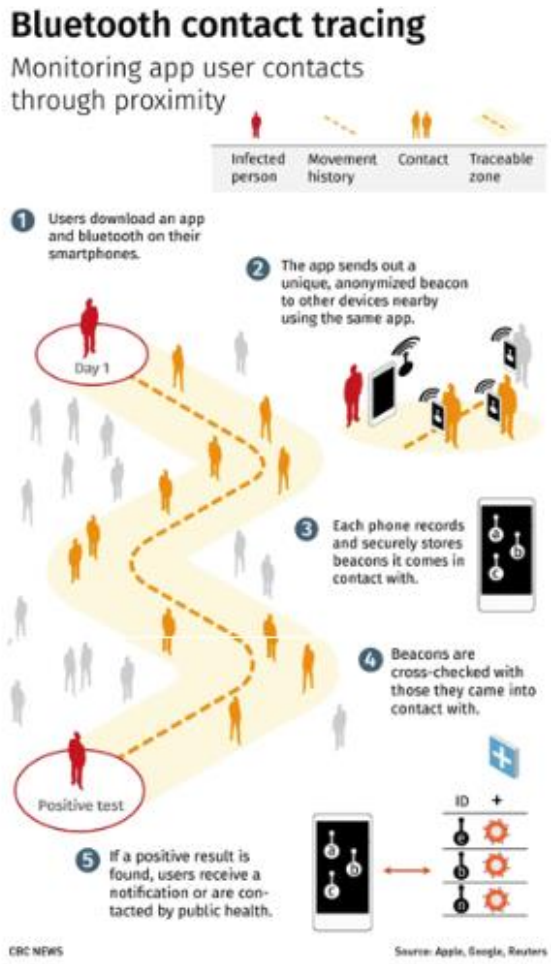
BLUETOOTH APPS: MONITORING USER CONTACTS THROUGH PROXIMITY

50. To log contacts between two users, Bluetooth apps use low-energy Bluetooth radio signals ("Bluetooth" or "Bluetooth Low Energy [BLE]"). In particular, they identify a person's contacts by swapping the phone's encrypted tokens with any other nearby phones, using Bluetooth[90] ("Bluetooth handshake"). More specifically, Bluetooth is used to emit and capture encrypted ID signals ("ephemeral identifiers [EphIDs]") from close-by mobile devices that also have an app, within a certain distance (e.g., X feet) and for a certain time (e.g., total X minutes over 24 hours).[91] "Both numbers are 'tunable' based on new data about how Covid-19 infections are occurring"[92] (e.g., app only obtains an ID number if an encountered person is within 1-2 metres/3-6 feet for a total of 15 minutes over 24 hours).[93]

51. Depending on the app, each mobile device holds a list of contacts for a set number of days[94] and, if a person tests positive for COVID-19, s/he "self-reports" to the app, which *either* (see infographic[95]):

    - uploads list of encrypted digital IDs so a PHA can notify and trace those who have been in contact with the infected person ("centralised Bluetooth app" [see details below]); or
    - transmits an alert directly to the apps of those on the list for those users to see[96] ("decentralised Bluetooth app" [see details below]) .

    Recipients of warnings are not informed who the infected contact was, and are expected to take appropriate steps (e.g., notify their doctor, monitor their health, isolate, or take a COVID-19 test).[97]



ARCHITECTURE: CENTRALISED & DECENTRALISED APPS

52. Based on their architecture ("data governance approach"[98]), contact tracing apps are distinguished into database-centric ("database-centric apps"[99] or "centralised apps"[100]) or event-driven architecture ("EDA") ("EDA-based apps"[101] or "decentralised apps"[102]).

CENTRALISED APPS

53. For centralised apps, data is captured and stored in databases, on central servers (aka "centralized database"), for subsequent processing and analysis.[103] These apps "routinely capture everything, so data can later be filtered for what's relevant and what's not".[104] If the central server is compromised, so is the entire network ("single point of failure").[105]

54. As noted, location-based apps are inherently centralised, whereas Bluetooth apps are not.

DECENTRALISED APPS

55. For decentralised apps, data is generally not captured and stored in databases (see proviso below), rather in "edge devices" (e.g., mobile devices).

"(S)ervices are distributed out to the edge (edge computers, intelligent sensors, handheld devices and the like). When an event is detected — an infected person entering a factory, a sensor detecting an impending flood or the signature sound of a gunshot — the processing and system actions are executed at the edge, immediately… (T)hese applications are truly real time and can respond to tens of thousands or even millions of events per second when required. What's more, they are smart enough to filter out extraneous data… And when the situation has been remediated, all the data associated with that event can be deleted from all of the edge devices."[106]

BLUETOOTH APPS (CENTRALISED/DECENTRALISED) MERIT CLOSE ATTENTION

56. As detailed below, at the global level, momentum has shifted from government adoption and deployment of geolocation to Bluetooth contact tracing apps, and the current battle is between the centralised model (losing) and decentralised model (winning). For this reason, centralised and decentralised Bluetooth CTAs merit closer attention.

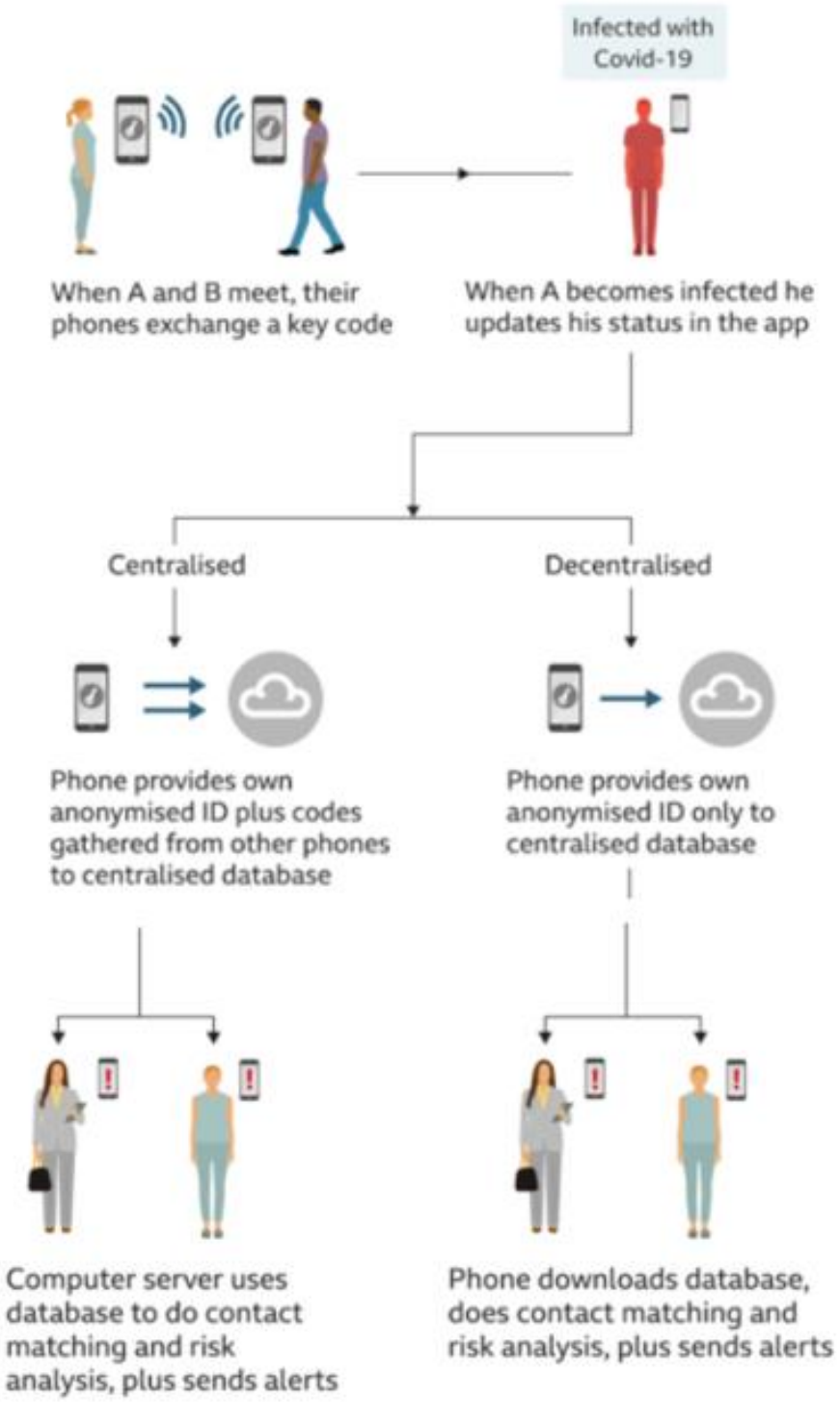
CENTRALISED V. DECENTRALISED MODEL

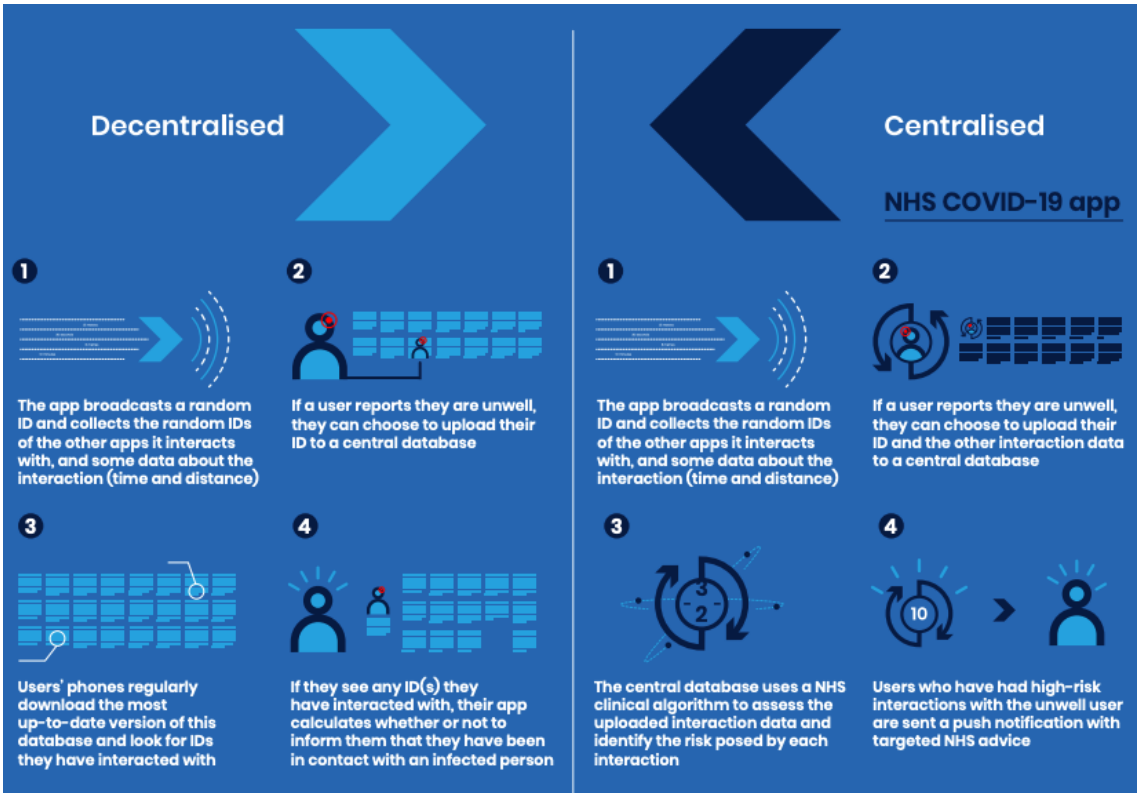
57. *Centralised* Bluetooth apps collect anonymised data and upload it to a central server, where contact matches are made.[107] "(T)he infected person uploads *both their own phone's ID code and the phone IDs of their recent contacts* to a central server. Although these IDs are anonymized, officials can see the entire network of contacts."[108]

58. In contrast, *decentralised* Bluetooth apps collect anonymised data and keep it on the mobile device, where contact matches are made.[109] "An infected user uploads *only their own anonymized ID* to a central database; all phones with the app regularly load the list of infected users to check for a match with phones they've recently been near."[110] As Wired explains: "When a user reports a positive Covid-19 diagnosis, their app uploads the cryptographic keys that were used to generate their codes over the last two weeks to a server. Everyone else's app then downloads those daily keys and uses them to recreate the unique rotating codes they generated. If it finds a match with one of its stored codes, the app will notify that person that they may have been exposed..."[111]

59. The centralised and decentralised infographics below are helpful, noting the first portrays an exposure notification app[112] whereas the second portrays a risk assessment app[113]:

Centralised v decentralised apps





60. There is a debate on whether the centralised/decentralised distinction is "truly meaningful".[114] Some experts emphasize that "(t)he real differences come down to this question of where the data is stored and where the matching is done", the central server or phones, "(a)nd those are true differences".[115] However, other experts argue "it (is) a false narrative to label one approach 'centralized' and another 'decentralized' because all systems would involve some information at the device level and some information *passing through* a common server".[116]

COMPETING PROTOCOLS FOR EACH MODEL

61. There are competing protocols (aka "frameworks" or "systems") for centralised Bluetooth models "centralised protocols") and decentralised Bluetooth models ("decentralised protocols").

62. **Centralised protocols.** The key centralised protocol is ROBERT (ROBust and privacy-presERving proximity Tracing protocol), developed by a group called PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) and initially led by German researchers[117]. It relies on pseudonymization and is not an autonomous system.[118]

63. **Decentralised protocols.** The primary decentralised protocol is the "Apple/Google Exposure Notification Application Programming Interface (API)" (aka "Google Apple Exposure Notification (GAEN) protocol"[119], "Google/Apple Exposure Notification API" or "Google/Apple API"). Competing protocols include: DP-3T (Decentralized Privacy-Preserving Proximity Tracing), an open-source protocol designed by a coalition of researchers from several European institutions[120]; TCN (Temporary Contact Number), a protocol designed by the TCN Coalition[121], specifically by its member Covid Watch[122]; and PACT (Private Automated Contact Tracing), designed by MIT[123] and UW[124]. The developers' collective aim is to provide different decentralised protocols that "can be adapted by countries depending on their local situation", and they are "committed

to working together to make their systems interoperate".[125] In particular, the TCN Coalition's mission is to facilitate interoperability between all decentralized protocols.[126] The DP-3T protocol, according to co-developer Michael Veale, was "adapted" by Google/Apple[127] and, according to some media reports, its developers are working with Google/Apple to ensure compatibility[128].

64. As detailed below, at the global level, currently the Google/Apple API is the winning protocol for decentralised Bluetooth apps. For this reason, it merits closer attention.

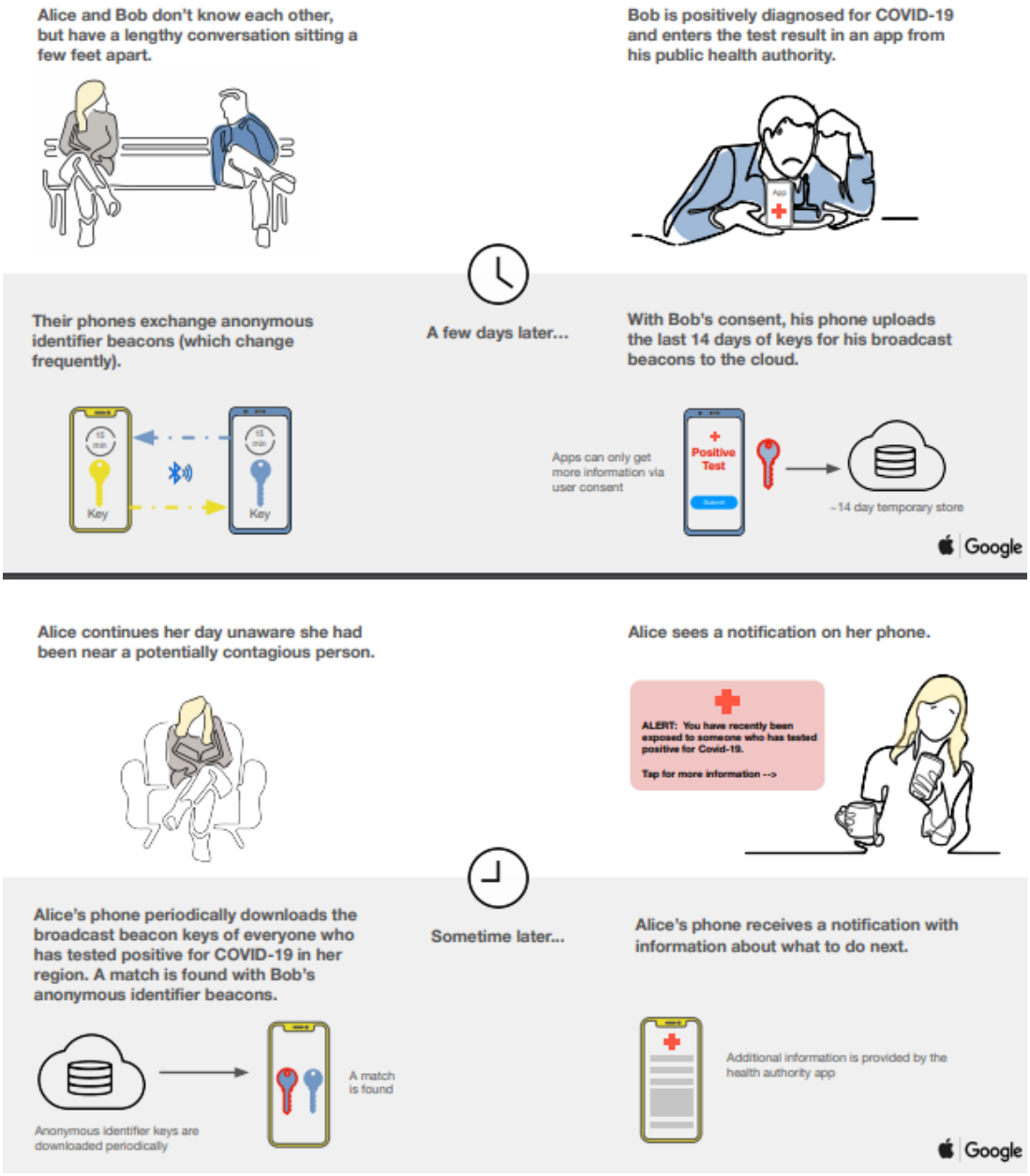
PRIMARY DECENTRALISED PROTOCOL: GOOGLE/APPLE API

65. **Google/Apple API.** The Google/Apple API is "only for official government health department apps that adopt a decentralized design"[129] (i.e., supports decentralised, official, PHA-developed apps[130]) and enables iOS and Android phones to communicate with each other over Bluetooth, allowing developers (PHAs) to build an app that works for both[131]. This is important because Apple/Google control 99.5% of operating systems.[132] The API has two phases:

- Phase 1: API released on May 20, 2020, for PHAs to incorporate into their own apps[133]. The API has since been updated, based on global PHA feedback.[134] For example, on July 2, 2020, Google and Apple's operating software updates added new privacy settings to the Bluetooth function called "COVID-19 exposure logging" that, when enabled by installing an authorized app on the phone, allows phones to exchange random IDs and notify users of exposure.[135] Other updates include changes to support interoperability between countries.[136]
- Phase 2: not yet released, it "will build the functionality directly into the operating system of both smartphone platforms" which "means users will not need to download a third-party app".[137]

"Apple-Google have repeatedly stressed that they have only created a tool, and it is up to public health authorities to develop, implement, and manage apps based on it as they see fit (within Apple-Google's strict guidelines, of course)."[138]

66. **How apps built on the API work.[139]** A mobile device with Bluetooth enabled and the app installed broadcasts a randomized number ("key") that changes every 10 minutes and records any keys it encounters that meet criteria set by app developers (PHAs) on exposure time (e.g., 15 minutes) and signal strength (e.g., correlated with a distance 6 feet away). All keys that are broadcast, received, or retained, are stored on the device in a secure database. An infected user (*presumed or confirmed*, at app developer's discretion) *can choose* to notify the app of her infected status, which broadcasts her keys to the network. Devices of other app users download the list of *infected keys* ("Diagnosis Keys") and check to see if any of them are in their on-device databases. If yes, they notify the user of possible virus exposure, reported in 5 minute intervals up to 30 minutes. The notified user – who does not know the name or any other personal data about the infected person – *can choose* what next steps to take (e.g., whether to self-isolate or get tested). The notified user's data does not leave her device, and PHAs cannot force the user to take any follow-up action. For a helpful Google-provided infographic[140], see below.



67. **API Terms of Service.** The Google/Apple API only supports certain apps or put differently, is subject to app restrictions or requirements that are set out in its Terms of Service ("Google/Apple API Terms of Service"[141]), including:

<u>App</u>

- as noted, official[142], PHA-developed (i.e., developed by PHA or PHA-authorized developers) ("PHA app"[143]), and decentralised
- one PHA app per jurisdiction, which includes one app per province or state[144]
- opt-in only (i.e., not mandated), for app and notifications[145]

- used only for purpose of "COVID-19 response efforts" and not for any other purpose (e.g., law enforcement, including enforced quarantine) except with user consent[146]
- provides notified users with guidance and resources[147] (required for Google, recommended for Apple)

Personal data

- *collection* not *required*[148], is the minimum amount of data necessary for COVID-19 response efforts and only with user consent (e.g., registration data may be collected with consent)[149], and complies with Google/Apple app stores' notice and consent requirements[150]
- *used and disclosed* only for purpose of COVID-19 response efforts except with user consent[151] but may not be shared with Google/Apple[152]
- *not used* in a way that would violate the legal rights of users, be associated with systematic discrimination or marginalization, or identify or facilitate identification of users who choose to not provide personal data[153]
- users are kept anonymous vis-a-vis (aka "identity is not shared with") *other users or Google/Apple*, however, as noted, PHAs may ask for personal data (e.g., phone number to contact users with additional guidance)[154]
- no "precise" location data[155]
- Diagnosis Keys (i.e., positive diagnosis) retained maximum 30 days from time of collection[156] (note: when user tests positive, their Diagnosis Keys are uploaded to the "Diagnosis Server", which aggregates the Diagnosis Keys from all users who have tested positive and distributes them to all users that are participating in exposure notification; if a user never tests positive, their Temporary Exposure Keys do not leave the device[157])
- API will be shut down once PHAs have COVID-19 pandemic under control[158]

Google Canada's head of public policy and government relations Colin McKay confirmed the API is designed in such a way that *app developers* can't request personal data, associate personal data with the Bluetooth information, or request *specific* location information.[159] PIAC notes the Google/Apple API Terms of Service identified above are inconsistent with certain media reports[160] that suggest there is a requirement that no personal data is relayed to PHAs.

68. The app developer (i.e., PHA or PHA-authorized developer on the PHA's behalf) is responsible for ensuring the app complies with the Google/Apple API Terms of Service and other relevant Google/Apple app store developer policies.[161] Further, the app developer is the "legal entity" that is "solely responsible for complying with applicable data protection and privacy laws and regulations".[162] The Google API Terms of Service expressly state that the app developer "in your capacity as *controller* of any personal data *processed* in connection with the use of your App, are solely responsible for complying with applicable data protection and privacy laws and regulations" and that the terms "controller", "personal data", and "processing" have the meanings given in the EU's General Data Protection Regulation[163] ("GDPR").[164] **The foregoing distinction is important, because it confirms that any Canadian official PHA app(s) built using the Google/Apple API must comply with *both* the Google/Apple API Terms of Service and Canadian privacy laws. Further, PIAC notes the Google/Apple API Terms of Service could require *more or less* stringent personal data protections than Canadian privacy laws, depending on what law(s) pertain.**

APPS HAVE BENEFITS & RISKS (INTRINSIC & EXTRINSIC)

69. DCTTs have benefits and risks (aka "pros and cons" or "opportunities and challenges") that are both intrinsic (i.e., inherent to technology design) and extrinsic (i.e., external to technology design). This section identifies the key benefits and risks of *contact tracing apps*, overall and specific to each app type.

OVERALL BENEFITS/RISKS OF APPS

BENEFITS: POTENTIAL TO STRENGTHEN PUBLIC HEALTH RESPONSE TO COVID-19 PANDEMIC

70. As noted, DCTT can *potentially* strengthen the public health response to the COVID-19 pandemic. For this reason, WHO encourages PHAs to evaluate DCTT "to contribute to the global knowledge base about new technologies in public health", using "standard performance indicators".[165]

71. However, to date, global deployment of *contact tracing apps* provides limited evidence of their effectiveness (see Part 3 for details).

RISKS: COST, TECHNOLOGY THEATRE, TECHNICAL, DELIBERATE ARBITRAGE, INEQUITY, SECURITY BREACH, SURVEILLANCE, PRIVACY/CIVIL LIBERTIES VIOLATION & PLATFORM POWER

72. **DCTT.** DCTT raises "technical, cost, and ethical issues", including "developer costs, hardware and software costs, training costs, and (need) for continuous user support" and "(e)thical issues surrounding privacy, security, transparency and accountability".[166] There is also a risk that DCTT, especially CTAs, will be viewed by policymakers as a substitute for a broader, strategic public health response to the COVID-19 pandemic, thereby exemplifying "technology theatre", defined as "use of technology interventions that make people feel as if a government — and, more often, a specific group of political leaders — is solving a problem, without it doing anything to actually solve that problem".[167]

73. **CTAs.** The key risks of contact tracing apps include:

- technical (i.e., functionality) and public health, which are inextricably intertwined (e.g., errors[168] [false positives or negatives])[169];
- deliberate arbitrage (e.g., using false reports of infections to harm others)[170],
- inequity (e.g., exacerbation of socio-economic divides, stigmatization, and discrimination, defined as unintentional or intentional disadvantaging of usually oppressed groups, in many forms, including increased scrutiny, denial of services, or additional unfavourable treatment)[171];
- in particular, subjugation of minorities and extra-legal societal controls, a belief reflected in J. Jackson's well-known judgment in *Railway Express Agency Inc.* v *New York*, 336 US 106, 112-113 (1949): "I regard it as a salutary doctrine that cities, states and the Federal Government must exercise their powers so as not to discriminate between their inhabitants except upon some reasonable differentiation fairly related to the object of regulation… (N)othing opens the door to arbitrary action so effectively as to allow those officials to pick and choose only a few to whom they will apply legislation and thus to escape the political retribution that might be visited upon them if larger numbers were affected. Courts can take no better measure to assure that laws will be just than to require that laws be equal in operation.";
- security breaches (e.g., insiders or hackers gain access to data)[172];
- mass surveillance[173] (government or private sector[174], temporary or permanent[175]);
- violation of privacy and civil liberties[176]; and
- platform power.

74. Privacy risks of contact tracing apps merit close attention.

PRIVACY RISKS MERIT CLOSE ATTENTION

75. The privacy risks of DCTT – especially CTAs – identified by global privacy experts are significant and numerous, including the following.

76. **Privacy risk #1 – voluntary but mandated-in-practice**: voluntary apps are mandated-in-practice[177], for example, by employers as a condition for returning to workplaces, whether on their own or as part of a package of "health and safety" surveillance measures (e.g., thermal scanners and wristbands) that further intrude on individuals' privacy. Harvard law professor Jonathan Zittrain refers to apps and broader "test/trace/isolate regimes" that are mandated by businesses and institutions (e.g., universities) as "the Company Town Model", and stresses that: "The overall regime may thus remain nominally a voluntary one, with respect to government coercion, but participation in private regimes like this will be by choice only in the sense that employees can quit their jobs, or students can choose to drop out of school, if they don't want to participate in their institutions' programs."[178]

77. **Privacy risk #2 – complex design and proprietary source code**: inhibits timely and verifiable review to ensure conformance with design specifications and pertinent privacy protection principles.[179]

78. **Privacy risk #3 – maximal functionality (maximal data, for maximal analysis):** data collected, shared, and stored is not only what is required for the primary purpose of contact tracing ("primary purpose" or "intended purpose") but also for secondary purposes.[180]

79. **Privacy risk #4 – untrusted data governance:** central data repositories (if any) are not trustworthy actors subject to public oversight (e.g., private sector data repositories)[181] or trustworthy actors (e.g., public sector data repositories) could share data with other government institutions (e.g., law enforcement, intelligence).[182]

80. **Privacy risk #5 – unsecured data**: no or low level of cybersecurity for the data-collecting device, the app itself, communication channels used to move data, and any central repository, as well as the absence of audits or monitoring to ensure no breaches occur or, if they do, are contained.[183]

81. **Privacy risk #6 – maximal data retention**: collected data is retained for longer than the lifetime of its primary purpose (e.g., data is not permanently deleted from the infected person's device, contacts' devices, or a central repository after that person's infectious period ends).[184]

82. **Privacy risk #7 – unprotected derived data and meta-data (which enable sensitive inferences about traced individuals):** derived data is used without consent and not protected by mechanisms to prevent re-identification and meta-data is collected, stored, or used in the analysis of contact traces[185]; anonymized data is de-anonymized by correlating it with other data sets[186]; reconstructed invasive information can include the "'social graph' of who someone has physically met over a period of time" and, with access to it, "a bad actor (state, private sector, or hacker) could spy on citizens' real-world activities".[187]

83. **Privacy risk #8 – improper disclosure and consent**: users are not made aware, in a clear and understandable way, what data is collected and how it is used (including disclosure of, and explicit separate consent for, any secondary uses), and disclosure/consent is not regularly renewed (to ensure ongoing need for tracing and users' ongoing commitment to participate)[188]

84. **Privacy risk #9 – no sunset provision**: no provision to automatically terminate data collection and delete stored data after the pandemic is deemed contained[189]

85. The *intrinsic* risks/benefits specific to each of type of app are examined next.

APP TYPE-SPECIFIC BENEFITS/RISKS

RISKS OF EXPOSURE NOTIFICATION, RISK AWARENESS & TRACKING APPS

86. **Technical and public health.** Risk awareness apps are described by proponents as the "best of both worlds" (i.e., exposure notification plus risk assessment) because "(e)arly awareness would reduce the number of contagious contacts and the rate of spread of the virus".[190] Tracking apps enable PHAs to be more reactive and preventative, by allowing them to: detect, issue rapid warnings about and responses to, and potentially

predict, high risk proximity *events*; and monitor and control *individual behaviour/mobility* (e.g., enforce government rules, such as physical distancing or quarantine) and *access to public spaces*.

87. **Privacy.** General consensus is that privacy risks are lowest with exposure notification apps and highest with tracking apps. However, in PIAC's view, risk awareness apps are equally as invasive as tracking apps, albeit in a different way: behavioural profiling as opposed to surveillance (monitoring) and location-tracking.

RISKS OF GEOLOCATION & BLUETOOTH APPS

88. **Technical and public health.** Location-based apps have technical problems, being "highly inaccurate"[191] or at least "lack(ing) sufficient accuracy"[192], because GPS technology is generally accurate only within a roughly 15-foot radius, therefore it is not sufficiently precise to gauge short distances between two phones to determine what contacts are most risky, and it can be obstructed (e.g., by buildings, trees and roofs).[193] Bluetooth apps by contrast can "achieve significantly more accurate distance measurements"[194] but have other technical problems, such as:

- unreliability[195];
- inaccuracy, because "signals can still degrade amid high levels of signal interference" (e.g., high-density buildings or streets)[196] and "Bluetooth signals that show the proximity of two individuals' mobile phones are not a certain indicator of infection risk — two people might be in the same space but physically separated, for example, by a wall"[197] or using masks[198]; and
- "an evidentiary void" due to the "lack of a well-defined 'epidemiologically significant contact period'"[199] (noting, again, that Bluetooth proximity is a proxy for physical proximity and distance is a further element of, or proxy for, risk of infection). "If for example, the virus remains aerosolized and lingers in the air longer than originally thought—as some scientists have argued—an app that only logs person-to-person interactions will miss infections that occur when an infected person leaves a room and another enters sometime later."[200]

A single app that is *both* location- and proximity-based is "an extremely powerful tool" that is more effective than apps that only do one or the other.[201]

89. **Privacy and security.** Location-based apps pose a privacy concern, because they can be used to expose personal data (e.g., user's home address, workplace, and routines) and, even if users' data is anonymized, "past research has shown that it is possible to reverse engineer anonymized datasets to reveal individual identities through a process of combining other data sources".[202] These apps also pose a security concern because use of individual location data "increases risks for users in the event of a cyberattack or data leak".[203] Bluetooth apps are "easier to anonymize and generally considered better for privacy than location tracking"[204], but they still have privacy and security risks:

> *"Because Bluetooth signals are broadcast openly, security experts warn about potential for wrongful surveillance of users' devices. There is a risk of bad actors actively monitoring and intercepting the signals of app users to identify those who are COVID-19-positive. It is then possible to reveal individual identities, for example on social media, to 'name and shame' individuals. [new para] Bluetooth technology is also vulnerable to spoofing and duping. In such cases, threat actors intercept the signals for the purpose of either omitting or falsifying data. For instance, someone could capture a user's signals and broadcast them to another location, making the user appear to be in two different places at once. Researchers have also found ways to intercept Bluetooth signals and either block or send bogus notifications, including false alerts telling users they have been in contact with an infected person."*[205]

RISKS OF CENTRALISED & DECENTRALISED APPS

90. **Privacy and security.** Decentralized apps generally pose fewer and less intrusive privacy risks than centralised apps (see details below).

RISKS OF BLUETOOTH APPS (CENTRALISED/DECENTRALISED) MERIT CLOSE ATTENTION

91. The risks/benefits of Bluetooth apps merit close attention, for the same reason provided above.

CENTRALISED v. DECENTRALISED MODEL

92. **Technical and public health.** Centralised apps *prima facie* don't work properly on iPhones due to Apple's Bluetooth restrictions (i.e., "Apple phones suspend use of Bluetooth scanning if the app is only running in the background"[206]).

93. The centralised model is more reliable, because "entit(ies) with access to the server" supervise the alerts and ensure that only users who are at risk are warned, thus minimizing false positives. Further, this model enables entities with server access to run analytics on the data, thereby giving insight into virus spread (an epidemiological argument) and app performance (a tracing argument). For example, it is easy for the entities to check whether the right people are getting notifications, because they can "see all the phones that got an alert and whether those users later reported symptoms or a positive test through the app" and "analyze Bluetooth handshakes that didn't lead to a notification because, for example, the contact was deemed too short"[207]. Based on this monitoring, "(i)f too many unnotified users (or not enough of the notified ones) get sick, the app needs tuning."[208]

94. In contrast, the decentralised model lacks reliability, thus maximizing false positives: "Without a central organization supervising the alerts, and making sure that only the users who are at risk are being warned, there is a risk that the app gets swamped in false positives and turns to complete chaos."[209] These false positives could come from: the above-noted Bluetooth technical issues (e.g., "Bluetooth leaks through walls, while viruses don't[210]); users self-diagnosing incorrectly (which can be fixed by only allowing users to report a positive diagnosis verified by a health care provider)[211]; or trolls (e.g., "'the performance art people will tie a phone to a dog and let it run around the park' to create canine contact-tracing chaos")[212]. The decentralised model's lack of a centralised entity to run analytics on the data diminishes insight into virus spread (epidemiological argument) and app performance (tracing argument):

> *"(H)ealth departments and researchers only learn about people who actually call in to report getting an alert. They can't see how many notified people they might be missing, which could make it harder to evaluate the app's accuracy and precision. Still, health departments can compare the attack rate for contacts they learn about through traditional interviews and through an app…As a rule of thumb, if the app's attack rate matches or exceeds that of the traditional method, 'we know the app is doing a really good job.'"*[213]

95. **Privacy and security.** *Both* Bluetooth models rely on encryption, thus posing security risks.[214] With the centralised model, a central database inherently creates security and privacy risks[215]. In particular, entities with server access potentially include PHAs and other government institutions, businesses, and researchers (public and private) – whether well-intentioned or malicious – with corresponding surveillance, security, and privacy implications (see details in Part 3). For example, a malicious actor could "join the dots" and use encrypted data to identify individuals.

96. There is an ongoing debate on whether the decentralised model offers a higher or lower degree of privacy and security than the centralised model. According to the decentralised model's proponents[216] and "hundreds of privacy, security and human rights scholars"[217], it offers a higher degree of privacy and security (see details below), albeit it is not privacy-proof because "the risk of a particularly snooping attack from a tech-savvy neighbour… can never be fully removed from any Bluetooth contact-tracing system"[218]. Opponents of the decentralised model, such as France's National Information Systems Security Agency ("ANSSI"), contend that it offers a lower degree of privacy and security, because: encrypted identifiers circulate on phones, which have phone-specific security settings; and the "interaction graph of individuals –

the social graph" could be reconstructed by "operating system makers" at the "operating system level on the phones" and by "the state…more or less easily depending on the approaches".[219]

COMPETING DECENTRALISED PROTOCOLS (ESP. GOOGLE/APPLE API)

97. **Overall.** Experts generally agree the Google/Apple API is "the most privacy-respecting"[220] of the competing decentralised protocols (which "meant reducing the efficacy of the apps based on their tool from a public health agency perspective"[221]) and while it "isn't perfect (…) many of the biggest concerns have solutions"[222].

98. **Technical and public health.** Key technical benefits of the Google/Apple API include enabling the app to run in the background of devices, thereby smoothing operation and saving battery life.[223]

99. **Privacy.** Key privacy benefits of the Google/Apple API include being fully opt-in[224] and only collecting data from users with a positive diagnosis, which is anonymized.[225] However, experts identify several privacy risks.

Risk #1: Google/Apple API Can Only Point Developers In The Right Direction

- The API "can only point developers toward the most privacy-preserving approach. Every app will need to be judged independently on how it implements that framework".[226] This pertains especially to location data and anonymous data (which "*could* still include IP addresses or other metadata that can allow for personal or location identification").[227] The World Economic Forum emphasizes that "Apple and Google's (…) system's reliance on IP addresses is a potential Achilles' heel that could open people up to the very sort of invasive tracking the project purports to be trying to prevent".[228]

Risk #2: Apps Build On Google/Apple API Will Inevitably Ask for Location Data

- The second Google/Apple API privacy risk is that apps built on the API "will inevitably ask for location data", at the very least *general* location data (e.g., what "country" or "region" users are in), either to enhance their effectiveness (e.g., by sending users only the Diagnosis Keys of new positive cases that are relevant to their area of movement instead of the worldwide database, which reduces the daily key download to just one or two megabytes) or because PHAs want more data to help better track infections.[229]

Risk #3: Implementation Of Google/Apple API Is Not Anonymous

- "While the system itself has anonymous properties, the implementation – because it's broadcasting identifiers – isn't anonymous".[230] It is uncertain "whether the upload can truly be anonymous, given how hard it is to move any data across the internet (sic) without someone learning where it came from".[231] For example:

  "Even if the keys that the app uploads to a server can't identify someone, they could, for instance, be linked with the IP addresses of the phones that upload them. That would let whoever runs that server—most likely a government health care agency—identify the phones of people who report as positive, and thus their locations and identities.[new para] Apps can prevent anyone other than the server from eavesdropping on those IP addresses and identifying diagnosed users by using HTTPS encryption and also padding data they upload to obscure it (…) But you still have to trust the app server itself not to collect and store identifying data from those uploads. [new para] The TCN Coalition and the Google/Apple project both say the server shouldn't collect those IP addresses as a matter of policy. But it's up to the app developer to follow that policy. [new para] In fact, many health care agencies will want to identify Covid-19-positive people. On that point, however, a representative from the Google/Apple project argued that trying to keep the Covid-19 status of infected patients secret from health care agencies themselves may be an unrealistic goal. After all, these are likely the same agencies administering Covid-19 tests. As such, the public has already entrusted them with identifying data about Covid-19-positive people."[232]

- Further, certain techniques (e.g., "correlation attacks" and variations on them) could reveal identities of infected users or help advertisers track them, albeit the latter is unlikely so long as advertisers continue to be denied access to the API.[233]

Risk #4: Implementation of Google/Apple API On Android Devices Collects Location Data

- On July 20, 2020, the New York Times reported[234] that for CTAs built on the Google/Apple API to work on Android devices, users must first turn on the *device location setting*, which enables GPS and may allow Google to determine their locations. Put differently, while the CTAs do not allow location tracking, "Google may determine and use the device locations of Android users of the apps, depending on their settings".[235] Google explains that since 2015, the Android operating system – pursuant to Google Play Services, which connects apps to other Google services (e.g., Google Sign In and Google Maps) – has required its device location setting to be enabled in order to scan for other devices using Bluetooth ("Android location requirement").[236] Once location is turned on, Google can determine users' precise locations, using Wi-Fi, mobile networks and Bluetooth beacons, through a setting called "Google Location Accuracy", and use the data to improve location services.[237]

- Google Play Services cannot be uninstalled and, if disabled, results in core elements of the operating system not working, including the exposure notification system that CTAs built with the Google/Apple API need to function.[238] However, according to Google, apps – including CTAs built with the Google/Apple API – that do not have user permission cannot gain access to the user's Android device location.[239] According to media reports "it is understood that Google does not have access to data within the app (…) nor does the app have access to the data gathered by Google Play Services"[240] and Google issued a statement to clarify that it "do(es) not receive information about the end user, location data, or information about any other devices the user has been in proximity of"[241].

Risk #5: Google/Apple API Could Be Changed In Future

- The final privacy risk of the Google/Apple API is that "at some time in the future Apple and Google might change the whole game in their own corporate interests by altering their standards".[242] In particular:

  ""So far, Google and Apple have been nothing but transparent in this situation, and they took the route of standardising and implementing the solution that was least invasive of people's privacy. But who knows if this gesture of goodwill might turn out to be a double-edged sword that could be wielded to justify new data-gathering standards or future abuse of data gathered, say, for example, so as to get to the stage where they can dominate the market in telemedicine?"[243]

100. **Platform power.** The Google/Apple API entrenches hardware and software "platform power", the "centralised control of computing infrastructure these firms have amassed", which is distinct from "the problem of privacy" and privacy enhancing technologies ("PETs") intended to solve it.[244]

> *"Using privacy technologies, such as 'federated' or 'edge' computing, Apple and Google can understand and intervene in the world, while truthfully saying they never saw anybody's personal data. Data is just a means to an end, and new, cryptographic tools are emerging that let those firms' same potentially problematic ends be reached without privacy-invasive means. These tools give those controlling and co-ordinating millions or even billions of computers the monopolistic power to analyse or shape communities or countries, or even to change individual behaviour, such as to privately target ads based on their most sensitive data — without any single individual's data leaving their phone. It's not just ad targeting: privacy technologies could spotlight the roads where a protest is planned, the areas or industries likely to harbour undocumented migrants, or the spots in an oppressive country most likely to be illegal LGBT clubs — not personal data, but data with serious consequences nonetheless. This approach is effectively what underpins the Apple-Google contact-tracing system. It's great for individual privacy, but the kind of infrastructural power it enables should give us sleepless nights. Countries that expect to deal a mortal wound to tech giants by stopping them building data mountains are bulls charging at a red rag. In all the global crises, pandemics and social upheavals that may yet come, those in control of the computers, not*

those with the largest datasets, have the best visibility and the best – and perhaps the scariest — ability to change the world (…) (D)eflating digital power isn't just about governing data: it's the walls of the underlying systems we have to tear down."[245]

101. In particular, Alexandra Dmitrienko, a professor of secure software systems at the University of Würzburg in Germany**,** believes "(t)he Android location requirement underscores a troubling power imbalance between governments and two tech giants that dominate the mobile market", in that countries using the Google/Apple API "have little recourse against the new global standards that the companies are setting for public health technology".[246] Massimo Zannoni, an electronic engineer in Zurich, contends that "with this app (i.e., CTAs built on the Google/Apple API) you're invited, by the government strongly appealing to your sense of responsibility and morality, to give away your live location to entities that are getting a profit out of it, in order to protect public health".[247] The Google/Apple platform power risk is revisited below, in Part 3.

102. With a thorough understanding of what DCTT is and how it works, it makes sense to identify and describe the current state of DCTT, globally and in Canada.

PART 3: GLOBAL DCTT – OFFICIALLY DEPLOYED (NETWORK & APPLICATION LEVEL), TEACHING IMPORTANT EARLY LESSONS (ESP. APPS ARE NOT A SILVER BULLET & PRIVACY RISKS ARE REAL & SIGNIFICANT)

103. Currently, at the global level, DCTT has been officially adopted and deployed, teaching important early lessons, especially that the above-noted inherent risks are real (not "just hypothetical") and significant. This is especially true for privacy risks, when they are considered in the context of broader geo-political trends.

DCTT (NETWORK & APPLICATION LEVEL) IS OFFICIALLY DEPLOYED

104. DCTT – both network- and application-level – has been officially adopted and deployed globally, in western democracies and authoritarian regimes, including jurisdictions where power is shared by national and sub-national governments.

NETWORK-LEVEL TRACING IS OFFICIALLY ADOPTED & DEPLOYED IN CERTAIN COUNTRIES

105. Network-level digital contact tracing has been officially adopted and deployed in certain countries, both democracies and non-democracies, alone (e.g., South Korea and Taiwan) or together with application-level tracing (e.g., China and Israel), and explored in others (e.g., US, UK, and Italy):

South Korea

- South Korea uses network-level data-mining only. Diagnosed infected people must describe recent movements, supported by data from GPS phone tracking, CCTV footage, and credit card transactions, then PHAs "send regional texts to alert residents in real-time, linking them to a website with further details on the case including their gender, age category, and names and addresses of the places they visited".[248] As of May 15, 2020, South Korea "has begun aggressively testing and tracing thousands of people who went to bars and nightclubs in Seoul after a cluster of new coronavirus cases emerged in its capital. Some of this tracing has involved *contacting telecom companies to gain location information* of people who were in those clubs to determine who might have been infected".[249] These measures enabled outbreak containment within 2 weeks, tracking down and tracing more than 45,000 people (of whom 160 tested positive). For additional details, see below.

Taiwan

- Taiwan enforces quarantine with location-based (cellphone triangulation) tracking: "If the person under quarantine ventures too far from home, it'll trigger an alert system which is followed up by calls, texts, and even an in-person visit by the police if the person can't be reached. Officials also call those in

quarantine twice a day to make sure they're close to their phones and haven't left home without it, while police conduct patrols at popular gathering places with a list of those who should be in quarantine. Anyone caught breaking the rules can be fined a hefty sum of up to NT$1 million (…)."[250]

China

- "China's tracking services are locally managed and employ disparate techniques, but all incorporate a number of parallel data streams that only such a robust authoritarian system could collect. Such streams include national databases that are tightly integrated with the private sector (…)"[251]

Israel

- TSPs shared location data with state agency security service Shin Bet for contact tracing (authorized until July 22, 2020 with no possible extension).

US

- As of March 2020, the White House was negotiating with major tech companies, including Google and Facebook, about potentially using location data that is aggregated and anonymized. Google stressed any government partnership "would not involve sharing data about any individual's location, movement, or contacts".[252] As of May 29, 2020, geolocation startup Camber Systems was building a network of aggregated location data ("Covid-19 Mobility Data Network") to help states and cities track citizens.

UK

- In March 2020, UK "telecom giant" O2 said it was one of a group of TSPs asked by government officials to share aggregate location data on mass movements, discussions are early stage, and it could build models that help to broadly predict the virus' spread. Further, the government tabled emergency legislation relaxing rules around intercept warrants.

Italy

- Italy sought anonymized, aggregated data from Facebook and TSPs to help with contact tracing and other forms of monitoring.

APPLICATION-LEVEL TRACING IS OFFICIALLY ADOPTED & DEPLOYED ACROSS REGIONS & MOMENTUM HAS SHIFTED TO DECENTRALISED BLUETOOTH (ESP. GOOGLE/APPLE API)

106. Global debate about official CTAs initially was technology-focused, on the proper type(s) of app, but has broadened to include policy issues, especially privacy (e.g., what personal data apps should collect and how much should be shared with PHAs). In many cases, this debate has taken place *after* initial official app adoption or deployment in a given country. Today, this debate – which reflects and reinforces evolving global government decisions on official app adoption and deployment – is focused on the two *Bluetooth* models, centralised and decentralised[253], with the latter, especially the Google/Apple API, emerging as the "winner", at least in democratic countries. Proof of these points is found in an overview of the current and still evolving state of global CTA adoption and deployment.

OFFICIAL APPS OF ALL TYPES ARE DEPLOYED ACROSS REGIONS (NATIONAL & SUB-NATIONAL LEVEL)

107. App-based digital contact tracing has been officially adopted and deployed across the world – starting in China (the source of the pandemic) as early as February 2020[254] – in Europe[255], Asia Pacific, the Middle East, Africa, North America, and Latin America. Official apps are:

- mandated (primarily in non-democracies [e.g., China], but also in certain democracies [e.g., India[256]]) and voluntary (primarily in democracies but also in certain non-democracies [e.g., United Arab Emirates]);

- exposure notification[257], risk assessment[258], and tracking[259] (with and without additional functionalities [e.g., immunity passports[260]]);
- location-based[261], Bluetooth[262], and location + Bluetooth[263]; and
- centralised and decentralised[264], including *Bluetooth* centralised and decentralised, with multiple decentralised protocols (including DP-3T [e.g., Estonia] and Google/Apple API [see below]).

108. Some official CTAs are stand-alone whereas others are accompanied by, or work together with, wearable devices, both mandated and voluntary (e.g., Australia, Israel, Bahrain, Singapore, Hong Kong, US)[265] and/or other digital outbreak response technologies (e.g., US Rhode Island's Salesforce-created database to assist manual contact tracing).[266] COVID-19 wearables are usually for the wrist or ankle (e.g., bracelet or ankle monitor) but also take other forms (e.g., "tokens" for carrying in a pocket or purse), have varying purposes *including but not limited to contact tracing* (e.g., early warning to identify COVID-19 patients, monitoring and enforcing social distancing, and enforcing quarantine), and use multiple technologies (e.g., electronic sensors to measure vital signs, GPS receivers, Bluetooth radio beacons, and QR codes).[267]

109. Some countries built their official apps from scratch, whereas others adapted apps developed by third parties, both government (e.g., Singapore's official app adapted by Australia) and non-government (e.g., Shopify-developed "COVID Shield" app adapted by Canada[268]).

110. A number of countries have not officially adopted or deployed apps at the national level (e.g., US[269] and South Korea). Of these countries, some have official apps at the subnational level (e.g., US) or unofficial apps are available (e.g., Uganda and Kenya).[270]

111. The result of these collective developments, across countries, is "emerging apps of many flavors"[271], both official and unofficial.

BLUETOOTH DECENTRALISED (ESP. GOOGLE/APPLE API) OFFICIAL APPS HAVE GLOBAL MOMENTUM

112. As noted, both *centralised and decentralised* Bluetooth models have been officially adopted and deployed. At the start of the pandemic, the centralised model was preferred by governments and "Singapore's TraceTogether was widely viewed as the one to emulate", but this has changed[272], and momentum has shifted to the decentralised model, especially the Google/Apple API[273]. Key reasons for the change include low adoption of centralised apps, primarily due to privacy concerns and technical issues, especially that centralised apps don't work properly on iPhones due to Apple's Bluetooth restrictions and Apple refuses to waive these curbs unless/until the apps align with the Google/Apple API (primarily, by converting to a decentralised model).

113. Some early adopters of the Bluetooth centralised model have switched to the decentralised model (e.g., the UK, which was developing its own centralized app ["NHSX Covid-19 App"], Germany ["Corona Warn App"); and Poland ["ProteGO"]). However, other early adopters of the centralised model are staying the course, including:

- India ("Aaroya Setu");
- Australia ("CovidSafe", based on TraceTogether);
- Norway ("Smittestopp"), which also collects location data, raising privacy concerns that could have contributed to a high drop-out rate and that resulted in its suspension (see details below);
- France ("StopCovid"), which deployed on June 1 with "strong doubts" about its compatibility with similar apps in other European countries[274] and is now "the only major holdout in Europe"[275]; and
- Singapore, which considered switching to the Google/Apple API but in June 2020 became one of the first countries to officially rule it out, primarily because "(t)he 'graph' would not be available to contact tracers" thus making it "less effective in our local context"[276].

Notably, France and Singapore tried and failed to convince Apple to help their apps work better on iPhone. France is also one of five (5) countries – including Germany, Italy, Portugal, and Spain – that issued a May 26, 2020 joint op-ed by top digital officials criticizing Silicon Valley for "imposing" standards on DCTT and calling for the EU to boost its "digital sovereignty" by gaining more independence from foreign tech companies (Apple and Google were not named).[277]

114. Meanwhile, the list of countries "flocking" to the Google/Apple API continues to grow[278], including launched apps in Austria, Croatia, Denmark, Germany, Finland, Gibraltar, Italy, Ireland, Japan, Latvia, Poland, Saudi Arabia, and Switzerland; as of August 5, 2020, apps are planned in another nine European countries (e.g., England).[279] Notably, this momentum is not evidenced in the US, where "despite early hype about the Apple-Google API", only Oklahoma, Alabama, South Carolina, and Pennsylvania plan to use it[280] and only Virginia's and North Dakota's apps have been launched[281].

115. The increasing number of countries using the Google/Apple API could make it easier to implement contact tracing when cross-border travel resumes and means that more technical experts are focused on solving the protocol's technical issues, which could have positive public health results (e.g., decreased false positives and negatives).[282]

GOOGLE/APPLE API OFFICIAL APPS DIFFER BETWEEN COUNTRIES

116. Official notification exposure apps built on the Google/Apple API differ between countries, regarding what happens after a user gets an alert[283]: Ireland's COVID Tracker app gives users the option to provide their phone number to PHAs to receive a follow-up call and has an optional symptom tracker to provide PHAs with information on how they feel (thereby helping PHAs "map" the pandemic); Germany's Corona Warn app advises users to seek medical advice; and Switzerland's SwissCovid app provides a hotline number to call.

ABSENCE OF GLOBAL COORDINATION UNDERMINES APP EFFECTIVENESS

117. **Absence of coordination (overall).** This discussion demonstrates the absence of global coordination of digital contact tracing, especially apps, which undermines the effectiveness of digital contact tracing, thereby negatively impacting public health. This is less of an issue when the borders of most countries are closed and more of an issue as and when borders re-open, because "you remove the ability to trace the virus as it crosses borders, and viruses don't respect borders"[284]. This inability to trace the virus at it crosses borders could impact the ability of citizens to travel between and within countries that have open borders, and the only workaround would be for users to download their destination country's app.[285]

118. **Different Bluetooth models/protocols.** Deploying different Bluetooth models *between and within* countries is suboptimal because "(t)here may be problems trying to make the two different types of system talk to each other"[286]. According to Dr. Michael Veale of the DP-3T group, "(t)he core reason is that centralised systems ask you to upload the people you have seen, and decentralised systems don't need that data, so they don't play well together".[287] Deploying *decentralized* Bluetooth apps with *different protocols* between and within countries is similarly problematic, unless the protocols are interoperable.

119. **Harmonization efforts.** Due to concerns about ineffectiveness resulting from the lack of global coordination, some supranational efforts to harmonize apps are underway. For example, the European Data Protection Supervisor ("EDPS") has called for an EU-wide app based on the Google/Apple API[288] and in June 2020 the EU published guidelines specifying a basis for compatibility of apps in different member states[289].

GLOBAL DCTT DEPLOYMENT, WHILE STILL EXPERIMENTAL, TEACHES IMPORTANT EARLY LESSONS

120. DCTT is still experimental, however its global deployment to date has taught important early lessons, including the following.

LESSON #1: OVERALL RISKS OF DCTT ARE REAL & SIGNIFICANT

121. The first lesson taught by global deployment of digital contact tracing technology (especially apps) is that its overall risks are real and significant. This is especially true for public health, technical, equity, and privacy and security risks, which are detailed below.

LESSON #2: PUBLIC HEALTH RISK – OFFICIAL APPS ARE NOT SILVER BULLET

122. The second lesson taught by global deployment of DCTT is that the effectiveness of CTAs is unproven. Key observations include the following.

DEPLOYED APPS HAVE LOW ADOPTION & LOW IMPACT

123. When Boris Johnson was berated in the UK Parliament for the government's abandonment of its original app, he replied: "I wonder whether the right honorable and learned Gentleman can name a single country in the world that has a functional contact tracing app—there isn't one".[290] According to experts, "Johnson's rebuttal is perhaps a bit reductive, but he's not that far off"[291], since "contact tracing apps have now been launched in many different countries and it's not clear that they've been a success anywhere that they've been launched".[292] Put differently, "No country has yet shown what an effective, widely adopted contact-tracing or exposure-notification app looks like."[293]

124. Country after country has seen low take-up".[294] As of August 5, 2020, the "world's most downloaded" CTA is India's Aarogya Setu (mandated in certain public places), with 100 million downloads. However, this is just 7.4% of the population and "(c)ountries with relatively smaller populations have managed greater penetration levels, including Singapore (37%), Australia, and Norway (26% apiece)".[295] Further, countries with deployed CTAs "have not reported them being particularly helpful"[296]. Indeed, "every large-scale deployer of contact tracing technologies — from Singapore to South Dakota, Iceland to Australia — has said that the technology hasn't made much difference".[297]

VOLUNTARY APPS DON'T HAVE ADOPTION LEVEL APPROACHING 60%

125. No country with a *voluntary* CTA has an adoption level approaching 60% (noting that Facebook, the most downloaded app in the US, has a 69% adoption rate).[298] Of countries with voluntary apps, Iceland had the greatest uptake (40%)[299] and the Republic of Ireland's app, launched July 6, 2020, appears to be "one of (Europe's) most successful apps" (downloaded 1.3M times in 8 eight days, representing over 26% of the population and about a third of the smartphone base, making it the fastest-downloaded app in Europe)[300]. In Western democracies, the adoption rate has generally been under 20%.[301] Further, data from Switzerland indicates that not everyone who downloads an official app actually uses it; as of August 10, 2020, its official app had over 2 million downloads but fewer than 1.25 million active users.[302]

126. Key reasons for low uptake of voluntary CTAs are "complacency" due to low infection rates[303] and low trust[304] resulting from technical, privacy, and security issues[305] (see details below), albeit there is some debate over which concern is primary, with some experts contending that while "(a)nxieties about privacy persist", "technical shortcomings in the apps deserve the lion's share of the blame"[306]. For example:

- A *combination of privacy and technical concerns and complacency* is blamed for low uptake of voluntary apps, as of July 21, 2020, in countries including Germany (Corona-Warn-App, "one of the most popular contact-tracing in Europe", estimated to have been downloaded by just 14.4% of the population), Italy (Immuni app downloaded by 7.2% of the population), and France (StopCovid, downloaded by 3% of the population, translating to just 14 exposure notifications being sent out since June 2).[307]

- *Privacy* concerns, alone or primarily, are blamed for low adoption rates of voluntary apps in other countries (e.g., Poland[308] and Norway[309]). Europeans "are increasingly concerned about how their personal data may be used, with whom it may be shared and the impact on their rights", the "spectre of stigmatisation (which) is already evident" and how "some of these increased collection measures will be 'rolled back' once the crisis ends, or indeed if they will be reduced at all".[310] Surveys of Americans are also telling. A June 2020 US survey conducted by Avira found that 71% of Americans would not download *any* contact tracing app if it were an option, citing privacy concerns as the main deterrent.[311] According to Avira's CEO, "these survey results send a clear signal to both app creators and the government" that apps "could fail before they launch if developers don't communicate to the public how they plan to protect people's privacy."[312] Avira concluded that "(b)ased on the study, 60% utilization of COVID contact tracing apps is highly unlikely".[313] On April 29, 2020, The Washington Post reported on a recent poll showing that nearly 3 in 5 Americans are unable or unwilling to use a contact-tracing app *built on the Google/Apple API*, primarily due to privacy concerns.[314] According to the Post:

  "A major source of skepticism about the infection-tracing apps is distrust of Google, Apple and tech companies generally, with a majority expressing doubts about whether they would protect the privacy of health data. A 57 percent majority of smartphone users report having a 'great deal' or a 'good amount' of trust in public health agencies, and 56 percent trust universities. That compares with 47 percent who trust health insurance companies and 43 percent who trust tech companies like Google and Apple."[315]

127. This discussion demonstrates there is "a circular problem": the *effectiveness* of voluntary apps "will inevitably influence whether people are willing to install them, while the number of people who install the app will directly influence its effectiveness", begging the question "(h)ow effective is effective enough for (people) to want to install" them?[316] In early May 2020, Microsoft Research crowdsourced a survey of Americans and found that: "(f)or every 1% it reduced the infection rate, Americans would be 5% more likely to install the app"; "more than 60% of Americans would install an app that reduces their infection rate by 50%, from 30 per 1,000 people to 15 per 1,000, and more than three-quarters of Americans would be willing to install an app that reduces their infection rate by 97%, to 1 in 1000"; and "an app must be able to accurately detect at least 50% of coronavirus exposures and must raise false alarms less than 10% of the time before most Americans will adopt it".[317]

THE MOST SUCCESSFUL COUNTRIES HAVE NO APP

128. Democratic "South Korea, seen as one of the most successful countries at tackling Covid-19, has done it *without a CTA*. It has however used other surveillance methods which would be seen as invasive by many"[318] (i.e., "an intricate location-tracking system" that includes a public database of infected persons, supplemented with location data from TSPs, and coupled with public websites that catalog infected persons' movements[319]). These methods are facilitated by a "bespoke legal regime – developed after its largely botched response to the 2015 MERS outbreak – that explicitly allows for aggressive public health surveillance."[320]

DEPLOYED APPS' SUCCESS DEPENDS ON PARALLEL MANUAL TRACING & TESTING

129. What success countries with *deployed CTAs* do have "appears to depend in large part on the availability and timeliness of testing capacity and (…) parallel manual contact tracing".[321]

IN COUNTRIES WITH HIGH ADOPTION OF APPS & OTHER DCTT, PHYSICAL RESTRICTIONS PLAY MAJOR ROLE

130. Even in countries with *high adoption of CTAs and other DCTT*, physical restrictions have played a major role because "there are potentially large amounts of asymptomatic transmission — meaning that no contact

tracing system can work without strong limits on movement."[322] For example, China's mandated contact tracing app and broader surveillance system "played a mere accompanying role" and "the main tool that helped to stamp out the virus" was "complete shutdowns of cities across the country".[323] On August 5, 2020, Livemint, one of India's premium business publications, reported its analysis of the MIT Technology Review's COVID Tracing Tracker database, which lists a total of 47 CTAs:

> *"Of the 30 countries for which complete data was available in the MIT database, 19 countries have registered at least 10,000 confirmed cases of coronavirus. Of the top 10 among these by app penetration, nine have shown a decline in rate of case growth since their app launch, as compared to the 30-day period before the app launch. Equally, a before-app and after-app comparison shows that seven of these 10 countries increased the severity of their lockdown. This includes high app-penetration countries such as Qatar (91%), as well as low app-penetration ones such as Indonesia and India (around 7%)."*[324] (Note: Qatar's app is mandated – see details below.)

WITH OR WITHOUT DCTT, RE-EMERGENCE FROM LOCKDOWN MEANS INCREASED INFECTIONS

131. "(T)here are no successful examples of re-emergence from lockdown without measurable increases in infections — *with or without contact-tracing technologies*".[325] Hong Kong was "the only place to have returned to public life without a significant increase in infections or a return to lockdown"[326], however in late June-July 2020 it announced new tight restrictions, short of a complete lockdown, to try to curb its "third wave" of infections.[327]

WITH OR WITHOUT DCTT, A STRONG PUBLIC HEALTH SYSTEM IS CRUCIAL

132. Finally, "the largest known indicators of COVID-19 deaths are health-system capacity, protective gear and worker safety — and there are a number of health systems that report shortages or vulnerabilities on all three fronts".[328]

133. This discussion demonstrates that contact tracing apps are not a "game-changer" or "cure-all".[329] Indeed, in the words of the MIT Technology Review:

> *"If contact tracing apps are following Garner's famous hype cycle, it's hard to avoid the conclusion they are now firmly in the 'trough of disillusionment.' Initial excitement that they could be a crucial part of the arsenal against covid-19 has given way to fears it could all come to nothing, despite large investments of money and time."*[330]

In light of this, digital rights groups claim that "some governments are using apps largely as performative gestures — to demonstrate to the public that they are taking some kind of concrete action against the virus".[331] Similarly, the Centre for International Governance Innovation ("CIGI") contends that global CTAs are "the breakout technology theatre hit of the COVID-19 response", evidenced by the fact "(t)here was a lot of attention paid to contact tracing apps at all political levels", focused on their technological details rather than their "questionable" role in responding to the virus or "harder questions about power and equity".[332]

LESSON #3: TECHNICAL RISKS – OFFICIAL APPS HAVE TECHNICAL PROBLEMS

134. The third lesson taught by global deployment of DCTT is that every type of contact tracing app has technical problems, including Bluetooth centralised and decentralised.

135. **Bluetooth centralised apps.** Bluetooth centralised apps have had technical problems. For example, Australia's app "has struggled mightily to log encounters between phones when one user's iPhone was locked; for some devices, the app worked only 25 percent of the time".[333] Singapore's app functions variably depending on minor differences in positioning (e.g., "when people sat across a table from each

other, signal strength was much lower if their phones were in their pockets than if they set the phones on the table" and sometimes the signal strength "increased as people moved farther apart—potentially because of reflection off of metal surfaces such as supermarket shelves") and does not work properly on iPhones due to Apple's Bluetooth restrictions.[334]

136. **Bluetooth decentralised apps.** Bluetooth decentralised (Google/Apple API) apps have also had technical problems (e.g., German users who haven't recently updated their iOS can't use the app).[335]

LESSON #4: INEQUITY RISKS – OFFICIAL APPS HAVE ACCESSIBILITY PROBLEMS

137. The fourth lesson taught by global deployment of DCTT is contact tracing apps have accessibility problems, prompted by technical problems and existing inequities (e.g., unequal access to the Internet and Internet-connected devices or the so-called "digital divide").

138. In some countries, the accessibility problem has been partly addressed by official adoption of wearables. For example, Singapore provides contact-tracing Bluetooth "tokens" that can be carried in a pocket or purse, and the first to receive them were vulnerable elderly people who don't own smartphones. Data cannot be accessed remotely, because tokens have no Internet or cellular capacity, so upon positive diagnosis, the wearer provides data (by handing over the token) to PHAs, who then conduct manual contact tracing.[336]

LESSON #5: PRIVACY RISKS – OFFICIAL APPS ARE PRIVACY-INVASIVE

139. The final lesson taught by global deployment of digital contact tracing technology is that apps – official and unofficial and location-based and Bluetooth (centralised and decentralised) – are privacy-invasive.

140. **Location-based official apps.** Qatar's mandatory *location-based tracking (plus Bluetooth)* app had a security flaw, now fixed, that put the personal details of more than a million people at risk.[337] In the US, the North and South Dakota *location-based tracking* apps ("Care19" renamed "Care19 Diary") was "found to be sending location data and a unique user identifier to Foursquare and Google, despite claiming not to share any data with third parties".[338]

141. **Centralised Bluetooth official apps**. As of May 20, 2020, cybersecurity experts had found seven security risks in the UK's *original centralised Bluetooth* app, including one that would allow hackers to intercept notifications that inform people they have come into contact with someone with COVID-19 to either block them or send out fake ones"[339]. Broader concerns were also raised about the government's contracts with tech giants (e.g., Palantir and Google), granting them access to NHS data, and about the UK's test and trace program as a whole breaching national data protection laws, because the government failed to carry out a legally-required privacy impact assessment ("PIA") ahead of launch.[340] On June 17, 2020, media reported that France's *centralised Bluetooth* StopCovid app had been found to collect the data of all people encountered by the user and not just those within 3 feet for 15 minutes.[341]

142. **Centralised Bluetooth + location official apps**. Norway's *centralised Bluetooth + location* app was criticized by Amnesty International as among the world's most privacy invasive (along with Bahrain and Kuwait)[342], "putting the privacy and security of hundreds of thousands of people at risk"[343]. On June 12, 2020, the Norwegian Data Protection Authority ("NDPA") (an EU-mandated independent public authority which investigates and enforces domestic violations of EU data protection laws) forced the Norwegian Institute of Public Health to suspend use of the app and delete all collected data after finding major privacy breaches that are *disproportionate* (e.g., due to low contagion levels). The breaches included location data collection, an improper solution for aggregating and anonymising collected data, and invalid consent because users who consent to data use for infection tracking purposes must also consent to data use for research purposes. On July 7, 2020, the NDPA formally banned all app-related processing of personal data.[344] "This is the first reported instance of a public health-sanctioned contact tracing app being suspended"[345], and

"conflict between the Norwegian agencies was viewed as a watershed event by many privacy experts and advocates, as privacy prevailed over public health concerns"[346].

143. **Decentralised Bluetooth (Google/Apple API) official apps.** The privacy risk posed by Bluetooth decentralised CTAs built on the Google/Apple ATI due to the *Android location requirement* has been recognized by some governments, such as Switzerland and Latvia, who unsuccessfully pushed Google to make a change (e.g., stop requiring Android users of CTAs to turn on location).[347] Some privacy experts recommended that absent a Google fix, the Irish government should consider listing Google as a "data controller" for the Irish app.[348]

144. **Unofficial apps – fakes and bad actors.** Google and Apple are "defacto regulators" of CTAs, "deciding which of the many developers can offer services in their (app) stores", and while "the main requirement for entry is proof of a relationship with a government entity or health-care organization (…) (t)here are still lapses."[349] In June 2020, US security researchers said at least a dozen fake "contact tracing" apps, designed to look like official apps and take advantage of their "brand recognition and perceived trust", have been deployed globally by "threat actors" to spread malware and steal user data.[350] A June 2020 study of over 100 contact tracing apps in the Google Play app store by the International Digital Accountability Council ("IDAC")[351] and an analysis by The Wall Street Journal found that some: are not transparent about collection, uses (e.g., potential advertising), and sharing of personal data; do not have a listed privacy policy (breaching Google's rules); share data (including location) with third parties; transmit location data and phone numbers without proper security, potentially exposing it to hackers; and ask for permissions that are potentially invasive and could collect more information than needed to accomplish the apps' core purposes (e.g., camera permission to take selfies without clearly explaining what use would be made of them).[352] IDAC president Quentin Palfrey said "'(w)e've seen some pretty bad privacy practices" and "(t)he fact that we have not yet observed those bad privacy practices translating into demonstrable ongoing harm doesn't mean that the harm isn't happening or might not be happening in the future.'"[353]

145. **Unofficial apps – businesses/employers.** According to BBC News[354], "(w)hile governments wrestle with data protection issues around app-based track-and-trace, many firms are planning their own schemes", including apps, wearables, and video surveillance. For example:

> *"Accounting giant PwC has developed an app called Check-In, which is being tested in its Shanghai office. Employees' mobiles register if they come into close proximity to co-workers. If someone tests positive for Covid-19, recent close contacts can be informed and asked to isolate. PwC expects to be able to market this to other employers. By contrast, start-ups including Locix and Microshare in the US, and Europe's Rombit, Estimote and Kinexon are among the many offering track-and-trace systems that don't need smartphones, but use wristbands and lanyards to monitor your physical location. Companies preferring video surveillance can turn to firms like Glimpse Analytics and Smartvid.io, which have adapted their artificial intelligence to see if workers are keeping their distance and even if they're wearing face masks. A few firms test their staff for the virus itself. Although it is an expensive approach, some offshore oil rigs, mines, and other confined worksites see this as the safest approach. Amazon has even said it's building its own testing facility. Much is still uncharted territory. For example, bosses might be tempted to use questionnaires to ask about who their workers live with, and what they do outside work, to identify any additional risks (…) While employees in theory aren't obliged to answer questions about their private lives, or agree to temperature or any other checks, given the 'imbalance of power' it isn't always easy to say no, especially at a time of high job insecurity (...) And firms can make complying with monitoring a condition of entering a building (…) Rombit, which originally developed wearable sensors for use at ports, says it has had more than 400 enquiries about an updated version to monitor social distancing. An electronics manufacturer in northern France has been using wristbands, issued by US firm Microshare, for the past month. They have identified three cases of the virus in that time, allowing them to send home anyone deemed at risk. UK hospitals, military facilities and prisons are piloting the same system (…) Like Rombit's, Microshare's system is anonymous unless someone tests positive for Covid-19."*[355]

Further, "COVIDPass", a global "health passport", is scheduled to launched in September 2020, with hopes it will become "a standardized solution for airlines, airports and border agencies", "eliminate quarantine for healthy travellers", "allow hotels, cinemas, theatres, sporting and concert venues to reopen safely" and "help restart the worldwide conference and exhibition industry".[356]

GLOBAL PRIVACY-INVADING CTAs MUST BE UNDERSTOOD IN CONTEXT OF BROADER GEO-POLITICAL TRENDS

146. The above-noted privacy risks are even more troubling when viewed in context of broader geo-political trends, including:

- techno-solutionist government responses to the COVID-19 pandemic (overall) that entrench Big Tech's[357] – the most valuable US-based technology companies, Amazon, Apple, Facebook, Google/Alphabet, and Microsoft ("Big Five" or "GAFAM")[358] – power and accelerate its push into the health sector, where it already has a privacy problem; and
- government support for medical big data initiatives to win the global digital health data race, with corresponding privacy problems for PHAs and private healthcare companies.

GOVERNMENT RESPONSES TO COVID-19 REFLECT & REINFORCE "TECHNO-SOLUTIONISM"

147. "Techno-solutionism" is the belief that technology should be the default response to every policy problem (health, social, economic, environmental, etc.).

148. Some experts argue the virus has unleashed a "feast" of techno-solutionism in terms of government responses to COVID-19, ranging from deployment of digital contact tracing technologies to relying on Big Tech companies (e.g., Amazon and Palantir) for infrastructure (e.g., contact tracing app-supporting Amazon Web Services ["AWS"] – see details below) and data modelling (e.g., UK NHS-Palantir data initiative, established to help hospitals prepare for heightened demand during the pandemic but now expected to outlive it[359]). In particular, these experts contend that digital contact tracing responses to the pandemic reveal "two strands of solutionism"[360], progressive and punitive, which could have long-term negative consequences:

> *"'Progressive solutionists' believe that timely, app-based exposure to the right information could make people behave in the public interest. This is the logic of 'nudging' (…) 'Punitive solutionists', by contrast, want to use digital capitalism's vast surveillance infrastructure to curb our daily activities and punish any transgressions (…) The worst is still to come: the pandemic will supercharge the solutionist state, as 9/11 did for the surveillance state, creating an excuse to fill the political vacuum with anti-democratic practices, this time in the name of innovation rather than just security".*[361]

149. Public-private partnerships on digital contact tracing technologies and data-related initiatives entrench the power of Big Tech and beg the question of how to structure Big Tech-government relationships in a way that protects against privacy violations and other abuses and ensures that the value of any pandemic-related data remains with government (not business).[362] This question is particularly important given the independent but pandemic-accelerated push of Big Tech into the health sector.

TECHNO-SOLUTIONISM ENTRENCHES BIG TECH'S POWER & PUSH INTO HEALTH SECTOR, DRAGGING ITS LONG-STANDING PRIVACY PROBLEM ALONG FOR RIDE

150. Big Tech has accrued profits and global power through mass collection and monetization of user data that it has long viewed as "the new oil":

"The trouble is we've been playing fast and loose with our personal data for the past decade. Our mobile phones are a treasure trove of valuable information for Big Tech. It knows where we are, our likes, interests and shopping habits, as well as our age, ethnicity, political allegiances and financial health. It keeps track of our family, friends and colleagues, our education and work histories, our biometric and medical data, and our photos and faces. Petabytes of data are bought and sold at extraordinary speed around the world to vast numbers of data brokers, adtech companies and internet giants. The Canadian data industry alone is estimated to be worth up to C$200bn — more than 10 per cent of our GDP. Much of this data is used, often in relatively transparent ways, to make money. So-called "free" internet services like Facebook and Google are now widely accepted as an exchange of service-for-data. The information generates revenue by allowing advertisers and adtech companies to target audiences more efficiently."[363]

151. Big Tech is increasingly moving into the health sector, where health data is a precious resource. This includes four of the "Big Five" companies – Amazon, Apple, Google (Alphabet) and Microsoft – which, prior to the pandemic, were already accelerating their pursuit of niche healthcare sectors: Alphabet "focusing on its AI expertise to drive precision medicine"; Amazon "shaping up to disrupt the pharmacy, virtual care, and telehealth realms"; Apple "knuckling down on clinical research initiatives via its wearables"; and Microsoft "focused on its race with Amazon and Google to lay claim to the healthcare cloud market".[364] At the same time, hospitals (public and private) are turning to Big Tech to store and analyze their patients' health data – including "cloud storage platforms managed by Amazon, Google, and Microsoft" – pursuant to "confidential data-sharing deals that leave patients in the dark about how the tech giants will use the information and protect their privacy".[365]

152. Big Tech's "forward march into healthcare"[366] complicates the legal issue of data ownership, since there are a multiplicity of potential owners, both government and business, and provides *all private players* in the healthcare space with a commercial incentive to collect and use as much personal health data as possible, for the cheapest cost. This is concerning, given Big Tech's track record of violating privacy outside the health sector. Illustrative examples follow.

153. **Google.** Google – which has amassed data about its users for nearly 20 years across multiple services (e.g., Google Search and YouTube) "fuelling one of the world's most successful advertising programs"[367] – faces a $5 billion lawsuit in the US for tracking "private" (i.e., "incognito mode") Internet use, alleging that Google gathers data through Google Analytics, Google Ad Manager and other applications and website plug-ins, including smartphone apps, regardless of whether users click on Google-supported ads.[368]

154. **Facebook.** Facebook collects and combines user data from its proprietary platforms (e.g., Facebook, Instagram, and WhatsApp, the three largest social media platforms in the world) and third-party websites "to build eerily accurate profiles that help advertisers better target users".[369] Although Facebook is not making inroads to the healthcare sector, it is responsible for what is perhaps the biggest data scandal of the Big 5: the Facebook-Cambridge Analytica data breach. This breach was disclosed by a whistleblower in 2018 and involved the harvesting of up to 87 million Facebook users' personal data, without consent, by Cambridge Analytica (through an app, downloaded by only 270,000 people) to target them for political advertising in the 2016 US election.[370]

155. **Google/Facebook.** A November 2019 Amnesty International report about Google and Facebook, entitled "Surveillance Giants"[371]:

- warned that Google and Facebook's data collection terms are a "Faustian bargain" requiring users to sign away their personal data and privacy right in exchange for "free" services and "the benefits of the digital world", thereby trapping them in "a system predicated on human rights abuses";
- stressed this "surveillance machinery" reaches beyond the platforms themselves, tracking people "across the web, through the apps on their phones, and in the physical world"; and

- called for a "radical transformation" of the tech giants' "surveillance-based business model", which has "abuse of privacy" at its "core" as "starkly demonstrated by (their) long history of privacy scandals" of which the Cambridge Analytica scandal was "the tip of the iceberg".

156. **Apple.** Apple has been accused of "empty grandstanding about privacy" since it enables and profits from "the surveillance that supposedly offends its values", such as "doing business with the biggest privacy offenders in the tech sector", for example: iPhone's web browser, Safari, by default routes web searches through Google and "those searches help funnel out enormous volumes of data on Apple's users"; and App Store distributes actually or potentially privacy-violating third-party apps (including Google's and Facebook's).[372] Critics argue that if Apple "really cared about personal data, (it) could take any number of actions to keep privacy violators off its platforms and away from its customers", for example: banning privacy-violating apps from the App Store or iPhone platform and regulating "free" data-hungry apps more aggressively.[373]

157. **Amazon.** Regarding Amazon, "(l)eaky AWS buckets have been responsible for a stunning amount of unwanted data disclosures in recent years".[374] In many cases, AWS data exposures result from hacks or mistakes enabled by its customers' defective or deficient security controls, for example: a 2017 leak of files from an unsecured database that exposed data of nearly 200 million US voters; and a 2019 leak via a misconfigured firewall of customer data from Capital One that impacted approximately 100 million people in the US and 6 million Canadians.[375] In such cases, Amazon's website about the cloud service absolves it of leak-blame, warning: "You choose how your content is secured".[376] This attempted disclaimer of legal liability was not enough to stop some US senators from calling on the Federal Trade Commission ("FTC") to investigate Amazon's role in the Capital One data breach, alleging that "Amazon continues to sell defective cloud computing services to businesses, government agencies, and to the general public" and thus "shares some responsibility for the theft of data".[377] Amazon subsidiary Ring, an Internet-connected doorbell/security camera, which has partnerships with almost 1,200 US law enforcement agencies, has also been the subject of privacy concerns. For example, a "stunning" data leak in December 2019 – "the latest in a string of incidents involving compromised Ring accounts" – exposed the personal information of over 3,000 Ring users, giving "a potential attacker access to view cameras in somebody's home" in certain cases.[378]

158. **Microsoft.** Microsoft is no stranger to personal data leaks. In its "latest breach", in December 2019, 250 million Microsoft customer records were exposed to the open Internet, for 25 days, including email and IP addresses, and locations.[379] Although personally identifiable information was generally redacted, the breach still presented a risk in term of scams (phishing and tech support).[380]

159. **Overall – cloud databases.** According to Threat Post, "cloud database misconfigurations – even by tech giants and cloud specialists – have become a bit of an epidemic"[381]:

> *"The most recent Microsoft data breach adds to almost weekly reports – at least since mid-2019 – of similar occurrences in large companies all over the world," Rui Lopes, engineering and technical support director at Panda Security, told Threatpost. "What's more, we know more than 50 percent of these incidents are caused by deliberate malicious attacks rather than human error – and they cost up to 27 percent more for that reason. Companies in any industry and of any size should build and implement solid data control strategies, allowing them not only to avoid direct financial losses but also the costly impact on reputation and client trust."*
>
> *The Verizon 2019 Data Breach Incident Report (DBIR) in May found that misconfiguration of cloud-based file storage accounted for a fifth (21 percent) of data exposures in the previous 12 months that were caused by errors. In all, cloud storage mishaps exposed a whopping 60 million records in the DBIR dataset."*[382]

160. Big Tech's privacy problem is reflected in low levels of individual trust, not only in the Big Five, but in all tech companies. These overall low trust levels are reflected in the above-noted low trust levels in Bluetooth decentralised (Google/Apple API) contact tracing apps related to privacy concerns.

161. Big Tech's push into the health market is not *only* a business decision (i.e., "not *just* to feed the databanks") but also part of "a marketing strategy that acts as a defence against antitrust investigations, screaming as it does that an attack on the tech companies is an attack on their ability to support health services".[383] According to Bianca Wylie, Senior Fellow at CIGI, "Canada's COVID app is now part of this unfolding global legitimacy and marketing exercise".[384]

TO WIN "GLOBAL DIGITAL HEALTH DATA RACE" GOVERNMENTS SUPPORT "MEDICAL BIG DATA INITIATIVES", WITH INCREASINGLY ELEVATED PRIVACY PROBLEM

162. According to KPMG, "in a new global healthcare data race, health systems – and economies – need to be careful they aren't left behind".[385] For this reason, governments are looking at "(h)arnessing health data for the national benefit" (health-related and economic), by supporting and subsidizing "medical big data initiatives", which is expected to earn significant clinical and financial return on investment.[386] These initiatives include digitizing and consolidating population health data to establish a national database that can be used by PHAs, other government institutions, businesses, and not-for-profit entities (e.g., researchers and academics).[387]

163. KPMG notes that "(u)nderstanding the true clinical and financial value of health data is (…) difficult when its future application is uncertain", however some countries (e.g., Israel and South Korea) have attempted to quantify it:

> *"Tellingly, Prime Minister Benjamin Netanyahu estimated that the country as a whole could earn as much as US$600 billion from the digital health market, representing a healthy return on their forward-thinking investment. The South Korean government is expanding subsidies and support for medical big data initiatives, consolidating its hospital data to establish a national database - including collecting genetic and biometric data for 10 million patients. Again, the goals are economic as well as health-related, with an aim to create 35,000 jobs in health and medical research and grow the country's share of the lucrative global bio and healthcare sector from the current 1.8 percent to 4 percent by 2022."*[388]

Further, KPMG emphasizes that quantifying the value of health data "depends on whether you are a patient, (health care) provider, industry, or government".[389] For the last three in that list, "(o)ne size won't fit all, so a range of transparent business models for intellectual property need to be agreed, in the form of data licensing, equity or revenue shares".[390] For the first, healthcare customers: "(a)n uphill battle is on the cards to convey the benefits of data sharing… to reassure them that they are the ultimate data owners… treated not as data assets to be exploited, but as co-players in the quest for improved healthcare."[391]

164. This battle to convey the benefits of health data sharing to citizens is complicated by global governments' and private healthcare providers' long-standing history of personal data breaches and accidental exposure. For example, in the US, a data breach at federal government website HealthCare.gov in October 2018 affected approximately 75,000 people, exposing personal data including names, birthdates, addresses, partial social security numbers, immigration status, employment information, and insurance plan details.[392] Over the past two years, 16 companies have gained paid access to de-identified patient data from the Mayo clinic through licensing deals that boosted the clinic's revenues and "generated crucial insights for health tech firms eager to commercialize digital products and services", without patient notification or consent.[393] This suggests that owners/operators of digital contact tracing technologies, particularly apps, could be incented to further seed the "burgeoning digital health industry"[394] with (possibly de-identified and aggregated) personal health data related to COVID-19. In Canada, a February 2020 GoC document tabled in the House of Commons revealed that at least 144,000 Canadians had their personal data mishandled by federal departments and agencies in 2018 and 2019, at 10 different departments and agencies, including Health Canada, which had 122 breaches that affected almost 24,000 citizens.[395] In December 2020, Canadian-owned company LifeLabs Medical Laboratory Services revealed the personal data of as many as 15 million Canadians had been stolen in a cyberattack.[396]

165. Experts have warned Canadians to "brace for a new era of cyberthreats", with increased size, scope, and magnitude, that happen simultaneously[397] and say health data can be more valuable than a credit card because it includes personal data (e.g., health card number or date of birth) with "unique value" that is stable over time and can be used to steal "health-care identities". [398] In mid-March 2020, the federal government's Canadian Centre for Cybersecurity ("CCCS") issued an alert about the heightened risk faced by health organizations involved in Canada's response to COVID-19, stating "sophisticated threat actors" could try to steal sensitive data on the response or intellectual property related to virus research and development.[399] LifeLabs is just one of a growing list of healthcare institutions, private and public, that have been victims of data breaches since May 2019, including "hospitals 'overwhelmed' by cyberattacks fuelled by (the) booming black market".[400] According to Raheel Qureshi, co-founder of cybersecurity firm iSecurity Consulting, the health-care sector is targeted more than any other industry in the country, yet: "(a) lot of health-care organizations are still in the middle of some kind of security road map, or they're starting the conversation now to understand, 'What do we need to do?' Banks started doing this 15, 20 years ago."[401]

GLOBAL TREND TO SACRIFICE PRIVACY FOR POSSIBLY INEFFECTIVE CTAS POSES DANGER OF "ORWELLIAN TRANSFORMATION" TO "BIG BROTHER WORLD"

166. Finally, some experts contend the global trend to sacrifice privacy in the name of permitting governments and their private sector partners to deploy digital contact tracing technologies that may or may not prove effective in protecting us from the COVID-19 pandemic is an "Orwellian transformation" that raises the post-pandemic prospect of a "Big Brother" dystopia even in liberal democracies already threatened by "surveillance capitalism" (defined as business-deployed surveillance technology to track and influence consumer behaviour).[402] These technologies, without independent oversight by privacy regulators, "can become seductive tools that governments will want to keep well beyond the containment of COVID-19".[403]

> *"Digital contact tracing seems like a smart and advanced technique that could keep us all collectively safe, but a Big Brother world is already under way in states with autocratic leaders. The risk of mission creep in liberal democracies with rising populist tendencies, as in parts of Europe and the United States, is real and urgent. Those who want to defend civil liberties will need to get ready for a public battle, to convince people, who may think sacrificing a bit of liberty is worth being able to leave their homes, that the time to fight for privacy is now; otherwise, we will no longer recognize our societies in a few years' time."*[404]

167. Further, these experts argue the seductiveness of contact tracing apps is particularly strong, thus requiring an elevated degree of concern and supervision:

> *"(W)hat matters in the long-term is which digital platforms will manage the applications after the pandemic has been brought under medical control, which public-private assemblages will have consolidated their power and profits, and which uses of health data will continue after the crisis. There is every reason to believe that the implementation of applications whose data are certainly anonymised during the process, but are later sent to interoperable systems, will finally connect the health data of individuals with police and border-crossing data identification systems. This is likely to integrate different spaces, from the most local (municipalities) to the transnational spaces of the global North (airports, train stations, etc.). This dystopian scenario needs to be rejected without ambiguity(…)"*[405]

168. How relevant is this danger in Canada? On July 30, 2020, The Logic reported on its survey of OPCC and all 10 PT privacy commissioners, to understand how their work has changed during the pandemic, as follows:

> *"The country's privacy commissioners shared the many challenges of their job during the pandemic, with* ***some worried that without proper oversight public and private bodies will use COVID-19 to increase surveillance****. All reported that the requests they were dealing with were mostly pandemic-related, and changing day by day, from health care to the collection of information at the border to contact-tracing apps."*[406]

169. Since the start of the pandemic, the Alberta Privacy Commissioner (Jill Clayton) has received approximately 250 assessments on the privacy implications of new virtual health-care practices and, according to a spokesperson, these reviews represent "an exponential increase in the number of virtual care solutions" being used in the province, which indicates "the challenges the health sector (is) facing" and also the broader challenges faced by all Canadian privacy commissioners in addressing the accelerated deployment of digital technologies (overall).[407] In a March 2020 blog post, Commissioner Clayton's office wrote: "security and privacy risks significantly increase when processes are interrupted, new processes are established or new tools are implemented during an emergency without proper planning or security and privacy controls"; and "(p)ublic health is the number one priority, but ensuring security and privacy risks are considered and mitigated to the greatest extent possible will help reduce other incidents from emerging during these challenging months ahead".[408]

170. The foregoing background information provides the context for the current state of digital contact tracing in Canada.

PART 4: CANADIAN DCTT – OFFICIALLY DEPLOYED (CTAs) & UNOFFICIALLY DEPLOYED (NETWORK LEVEL) BUT STILL EVOLVING

171. Currently, the nutshell state of digital contact tracing in Canada is: officially deployed (application level) and unofficially deployed (network level), but still a work in process, and the situation continues to evolve rapidly. A detailed description of the current state of digital contact tracing is provided next. To provide necessary Canada-specific context, this discussion begins with a brief overview of government jurisdiction over the COVID-19 pandemic response and contact tracing (overall).

JURISDICTION OVER COVID-19 PANDEMIC RESPONSE, INCLUDING CONTACT TRACING, IS SHARED BY FPT & MUNICIPAL GOVERNMENTS

172. Jurisdiction over public health is complex and must start with a terminological distinction.

173. **"Public health" versus "public health-care".** It is important to distinguish between "public health" (aka "public health system" or "public health services") and "public health-*care*" (aka "the public health-care system", "health-care system", or "health care").[409] According to GoC, "(b)oth work to limit the impacts of disease and disability", however public health "involves the organized efforts of society to keep people healthy and prevent illness and premature death", "is a combination of programs, services and policies that protect and promote the health of Canadians", and "targets entire populations to keep people from becoming sick or getting sicker" whereas public health care "focuses mainly on individuals".[410] In the rest of this document, "public health system" and "public health-care system" will be specified where meant.

174. **Jurisdiction over public health and public health-care.** According to GoC, federal, provincial/territorial, and municipal governments "share responsibility for *public health*", however "different levels of government are responsible for different aspects".[411] Municipal (aka "local") governments "have primary responsibility for responding to *public health emergencies* in their jurisdictions"[412], however:

> *"If a public health emergency grows beyond a municipality — either in terms of the municipality's boundaries or its ability to deal with the emergency, then the provincial or territorial governments may be asked to step in and provide assistance. If a public health emergency grows beyond one province and/or territory — again, either its boundary or capacity, the Public Health Agency of Canada ("PHAC") usually gets involved — often playing a coordinating role. This can also include lending its lab capacity, contributing from emergency medical and equipment stockpiles and response teams, and connecting with the World Health Organization ("WHO") and other countries."*[413]

For this reason, "(a)ll levels of governments have various forms of legislation to protect and manage public health in a time of crisis".[414] In particular:

Overall

> *"Emergency measures and emergency management at the federal level in Canada are regulated by the Emergency Act and the Emergency Management Act. However, there is a relatively high trigger for the federal government to take the lead in a health emergency. Therefore (…) (m)ost provinces and territories have passed various 'health acts' that govern the powers and duties of health officials during a health emergency (…)"*[415]

Federal

> *Canada's federal legislation also includes the Quarantine Act, the purpose of which is 'to protect public health by taking comprehensive measures to prevent the introduction and spread of communicable diseases.' The Canada Border Services Agency (CBSA) assists the PHAC in the administration of the Quarantine Act and the Quarantine Regulations. The Act is by and large a border-control statute that is applied at entry and departure points."*[416]

Provincial/territorial

> *"Public health activities, including public health crisis management at the provincial and territorial levels, are governed by Public Health Acts (or their equivalent) and related regulations. These Acts usually have provisions on reporting requirements, prevention, inspection powers, emergency measures, and the powers and duties of health officials. [new para] Provinces and territories also have Emergency Management Acts in their respective jurisdictions that provide the legal basis for establishing emergency management organizations (EMOs) and creating provincial/territorial-level emergency management plans to help coordinate a provincial response to an emergency."*[417]

175. The constitutional power over *public health-care* primarily belongs to PT governments. Canada has a government-funded health care system ("Medicare"), however instead of a single national plan, there are 13 PT health care insurance plans, which must be administered and operated on a non-profit basis by a public authority.[418] The federal government provides health care funding to PTs through the Canada Health Transfer ("CHT"), sets and administers national health care standards through the *Canada Health Act*, and provides other health-related functions (e.g., disease monitoring/prevention).[419] PT governments are responsible for managing, organizing, and delivering health care services to their residents.[420]

176. **Jurisdiction over COVID-19 pandemic response and contact tracing (overall).** Flowing from this discussion, federal, PT, and municipal governments share responsibility for responding to the COVID-19 pandemic, however the federal government's role with respect to contact tracing (overall) is effectively limited to coordination.[421]

177. **Public health system and PHAs**.[422] The public health system involves PHAs, as defined above. For purposes of the privacy analysis that follows, it is important to identify the key PHAs at each level of government:

- Federal PHAs: Canada's Health Portfolio, headed by the Minister of Health, which includes a department (Health Canada) and agency (PHAC), which is supported by a Canada-wide network (Pan-Canadian Public Health Network ["PHN"]) comprised of "federal, provincial and territorial public health leaders and select public health partners (e.g., the Canadian Public Health Association)".[423] As noted, PHAC collaborates with similar global and national organizations (e.g., US Centres for Disease Control ["CDC"]).[424] The Chief Public Health Officer ("CPHO") leads national public health matters, provides advice to the Minister of Health and PHAC President, and works with other federal departments, and PT and municipal governments, amongst others.[425] GoC also operates the Canadian Network for Public Health Intelligence ("CNPHI"), an online platform accessible by authorized FPT PHAs, for "fostering collaboration and consultation through innovation in disease surveillance, intelligence exchange, research and response to protect, promote and support public health".[426]

- PT and municipal PHAs: PT chief medical officers of health and local chief public health officers/chief medical officers of health.

POLITICAL DEBATE ON DCTT STARTED AFTER INITIAL DEPLOYMENT & FOCUSED ON PROPER OFFICIAL APP LEVEL & TYPE

178. A political debate between and within the federal, PT, and municipal governments about digital contact tracing *technologies*, focused on the proper *level and type(s) of app,* started – or at least publicly surfaced – *after* initial deployment of digital contact tracing technologies – official and unofficial – at the application level (i.e., May 1, 2020, launch of Alberta's official contact tracing app "ABTraceTogether"[427]) and network level (e.g., Telus-Natural Sciences and Engineering Research Council of Canada ["NSERC"] database agreement[428]). The substance of this political debate is detailed below. **PIAC believes that starting the political debate on DCTT after its initial deployment is neither transparent nor democratic and that it is contrary to both the rule of law and privacy law.**

CANADA'S NATIONAL STRATEGY FOR OFFICIAL APPS WAS NOT UNIVERSALLY SUPPORTED BY PT GOVERNMENTS

179. On March 24, 2020, Prime Minister ("PM") Trudeau said "all options are on the table to do what is necessary to keep Canadians safe in these exceptional times".[429]

180. In May to early June 2020, PM Trudeau:

- emphasized the importance of contact tracing (overall) and that GoC wants to work closely with PT governments on it, offering volunteers and financial support for manual tracing efforts;
- stated GoC is working with "a number of different partners" (including Google/Apple) on potential contact tracing apps, *hopes Canada will adopt only one*, intends to "recommend strongly to Canadians a particular app", and expects a "clearer picture" on this decision in June 2020; and
- stressed that once the app is chosen, Canadians will be "strongly" advised to download it.[430]

This GoC approach effectively constitutes a national strategy for contact tracing apps ("National Strategy for CTAs").

181. The National Strategy for CTAs aligns with the public position of some PT governments, whose Premiers had previously called for a national strategy (e.g., Ontario and Manitoba).[431] It also aligns with the recommendations of certain Canadian privacy experts (e.g., Ann Cavoukian, Executive Director of the Privacy & Security by Design Centre and former Ontario Privacy Commissioner, and Teresa Scassa, Canada Research Chair in Information Law and Policy at the University of Ottawa) who support a national strategy on grounds that if PT and/or municipal governments decide to go their own ways, their respective official apps could be incompatible, which would decrease their effectiveness: "Think about Ottawa, where you have the city, the province and Quebec (adjoining). If Ottawa adopts one app, the province of Ontario adopts a different app and Quebec adopts its own app and people are moving across the borders every day and they're not interoperable, they're not collecting complete or reliable data about contacts."[432]

182. According to federal Health Minister Patty Hajdu, as of early June 2020 there was pushback on the National Strategy for CTAs from some PT governments who "prefer" doing contact tracing "the old fashioned way" (i.e., manually).[433] Minister Hajdu questioned "the usefulness of an app if there is not a high take-up" but also suggested that PT-specific apps could be bridged together, somehow.[434] This pushback continued beyond GoC's announcement of an official national app (see details below).

CANADA HAS AN OFFICIAL NATIONAL APP ("COVID ALERT" OR "COVID ALERT CANADA") FOR OPTIONAL ADOPTION & CUSTOMIZATION BY PT GOVERNMENTS

183. Canada has an official national contact tracing app for optional adoption and customization by PT governments.

GOC ENDORSEMENT OF COVID ALERT CANADA & ONTARIO ADOPTION ("COVID ALERT ONTARIO"): 18 JUNE 2020

184. On June 18, 2020, PM Trudeau announced GoC's adoption of a national, "completely voluntary" *Bluetooth decentralised (Google/Apple API) exposure notification* contact tracing app, developed by the Canadian Digital Service ("CDS") and the Ontario Digital Service ("ODS") – respectively the in-house digital development wings of GoC and the Ontario government – "working with"[435] Shopify (no details) and Blackberry (security review), and customizable by PT governments, to be released first in Ontario ("June 2020 PM Trudeau announcement").[436] The PM did not announce the official name of the national app[437], however it was subsequently confirmed to be "COVID Alert", mirroring the announced official name of the Ontario app.[438] To distinguish between these apps for analytical purposes, this document refers to the national app as "COVID Alert Canada" and the Ontario app as "COVID Alert Ontario".[439]

185. **Built on Shopify's COVID Shield**. According to a GoC source, "the national and Ontario apps are distinct, but both are based on COVID Shield"[440], an open-source, *Bluetooth decentralized (Google/Apple API) exposure notification* app developed by volunteers from Shopify to be used by PHAs in any country, free of charge, to build their own app (see dedicated website: https://www.covidshield.app/).[441] As of July 27, 2020, developers seconded from Shopify to GoC were working with CDS and ODS to solve issues with COVID Alert Canada's underlying Google/Apple API and integrate PT health systems.[442]

186. **PT involvement.** At the time of the June 2020 PM Trudeau announcement, he explained that "a number of other provinces, including BC" are "working with"[443] GoC on COVID Alert Canada, which will be customised for each PT that *chooses* to adopt it. Deputy PM Crystia Freeland confirmed that it will be up to each PT and its local PHAs to decide whether or not to adopt the app, and GoC sources confirmed the app will work in all PTs, even those that don't adopt it.[444] GoC "particularly liked the integration (of the app) with local public health officials"[445], according to an Ontario government source, and Minister Hajdu emphasized the app "will complement other public health measures to limit outbreaks of COVID-19, including testing and contact tracing".[446]

LAUNCH OF COVID ALERT CANADA & COVID ALERT ONTARIO: 31 JULY 2020

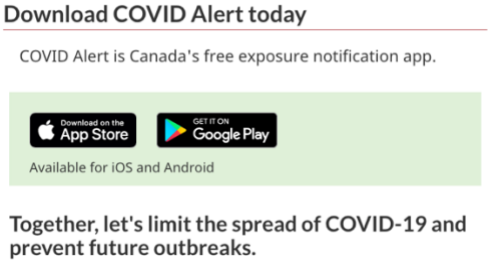
187. **Delayed launch (July 2, 2020).** COVID Alert Canada was initially scheduled to launch on a test/pilot basis in Ontario on July 2, 2020, and to launch nationally later in July 2020[447]. However, the Ontario rollout was delayed for reasons that were not initially specified by GoC.[448] Minister Hajdu later said the reason was to "make sure that the app was tested and thoroughly debugged" to ensure user-friendliness and because GoC was working "very closely" with OPCC to be "fully cognizant of how best to protect Canadians privacy".[449] Additional reasons were provided by non-GoC sources, including GoC's desire for a federal server (unnamed Ontario government official) and GoC's attempts to sign up other PTs (Ontario Premier Ford).[450]

188. **Beta test (July 21, 2020).** On July 21, 2020, CDS announced the start of a beta test, lasting 2-4 days, with a notice stating "(w)e're testing the app and not you"[451] ("COVID Alert Canada test phase") and a proviso that "(y)our participation and answers will not affect your access to Government of Canada services or benefits"[452]. According to CDS CEO Aaron Snow, "nearly 6,000 people (…) helped us improve the app by testing it".[453]

189. **Launch (July 31, 2020).** On July 31, 2020, COVID Alert Canada launched in Ontario and nationally, with a dedicated GoC website[454] ("COVID Alert Canada website" or "GoC website" – see screenshot). However,

"Ontario is the first province where people can use (it) to report a COVID-19 diagnosis"[455]. For an overview of the apps' features, see below.

190. **Adoption by other PTs.** At the time of the launch, PM Trudeau said that other PTs "will be joining in soon"[456], the Atlantic PTs will be next to officially adopt the app, and discussions with other PTs are ongoing[457]. The GoC website emphasizes that until all PTs officially adopt the app, "it's still helpful to download" it outside Ontario because "when people in your area are able to report a diagnosis, you'll be notified if you were near them".[458] GoC has not yet determined how to onboard Canadians who obtain health care from the federal government (e.g., First Nations people living on reserves, Inuit, serving members of the military, eligible veterans, and some refugee claimants).[459]



191. On August 7, 2020, federal Digital Government Minister Joyce Murray confirmed that GoC "expect(s) that all the provinces and territories will be part of this in due course"[460] and, on August 8, Alberta said it would officially adopt the app (timing TBD and up to GoC)[461]. This means that only two of the thirteen PTs (15%) have signed on.

192. **Adoption target for Canadians.** Canada has a population of nearly 38 million (with Ontario accounting for the highest populated PT with over 14 million residents) and, according to PM Trudeau, "there are over 30 million smartphones that could take this app in Canada".[462] However, neither GoC nor Ontario has announced a formal app adoption target. During the June 2020 PM Trudeau announcement, he said COVID Alert Canada "will be most effective when as many people as possible have it"[463] but "any level of uptake would be useful" and at 50% or more "it becomes extraordinarily useful" because "it'll actually allow us to have a better sense of when there are spikes or resurgences of a virus in a particular area or not"[464] (because local PHAs will get calls from users who have received notification alerts)[465]. When the PM announced the app's launch, he added, "(i)n fact, health experts say that if enough people sign up, this app can help prevent future outbreaks of COVID-19 in Canada".[466] On August 7, 2020, Minister Murray confirmed there is not a particular threshold below which GoC considers the app to be ineffective.[467]

193. According to Minister Murray, GoC will spend up to $10M on a public awareness campaign to boost downloads of COVID Alert Canada, including "advertising and outreach to key stakeholders", complementing PT governments' promotional efforts and the plans of Google, Apple, and "a variety of retail organizations" to promote the app, free of charge.[468] GoC's post-launch media campaign to drive adoption includes websites and social media platforms[469] and its key message is that downloading the app "helps you protect your loved ones " and "protect your community" by "limiting the spread of the virus and preventing future outbreaks" (for example, see tweet below).

194. **Privacy assessment.** At the time of the June 2020 PM Trudeau announcement, he recognized that adoption of COVID Alert Canada will depend on how Canadians' privacy and security concerns are addressed, describing the app as one that Canadians can download and forget about[470], promising it is "totally secure" and "the privacy of Canadians will be fully respected"[471], and asserting that in developing the app, GoC consulted with OPCC[472] (a claim that OPCC disputed in a statement later that day[473]).

195. The launch of COVID Alert Canada was accompanied by an explicit Privacy Notice[474] and a positive but qualified privacy assessment by OPCC and the Information and Privacy Commissioner of Ontario ("Ontario Commissioner" or "IPC")[475], based on a privacy self-assessment by Health Canada[476] ("Health Canada Privacy Assessment").[477] The Canadian and Ontario Commissioners found the apps met the "key privacy principles outlined in a joint federal, provincial and territorial statement on tracing applications"[478] (i.e., the May 2020 Joint Statement by FPT Privacy Commissioners – see details in Part 5) but made a number of "final recommendations" to "further enhance the privacy and security protections", which Ontario "has already committed to addressing"[479]. Privacy Commissioner Therrien said "Canadians can opt to use this technology knowing it includes very significant privacy protection" and "I will use it".[480] Health Canada said it expects the "privacy-first approach" of COVID Alert Canada, combined with the above-noted "strong communications and marketing strategy" will "significantly increase the number of users downloading the app than has been the case in countries that launched such programs in earlier phases of the pandemic".[481]

196. Canadian privacy experts generally expressed support for COVID Alert Canada[482] and encouraged Canadians to download it. Expert and media criticism of the app generally focuses on accessibility issues.

197. **Mandated use by third parties.** Pursuant to current Canadian law, third parties are permitted to mandate – as a condition to access services, benefits, or employment – the use of COVID Alert Canada or access to information in the app (e.g., whether the user has received an exposure notification). The OPCC and IPC "final recommendations" include finding ways to *eliminate* the "risk that third parties may seek to compel app users to disclose information as to their use of the app".[483] On August 7, 2020, Minister Murray would not commit to legislation that would prohibit third parties, specifically municipal governments and businesses, from mandating the app's use,[484] stating "(i)t is not for the government to be dictating what other private-sector or public-sector organizations are using as their criteria for providing service".[485]

198. **Potential additional or alternative official CTAs (national and/or PT).** The existence of COVID Alert Canada does not preclude GoC's *future* endorsement of additional or alternative national CTAs, of which both have occurred in other countries.[486] It is also possible that PTs could decide to adopt COVID Alert Canada and/or other apps (see details below). For this reason, PIAC believes all current and future *unofficial* CTAs should be viewed as potential official CTAs and, if they remain unofficial, as potential tools for use – transparent or non-transparent – by government institutions, private sector organizations (businesses and non-businesses), and not-for-profits.

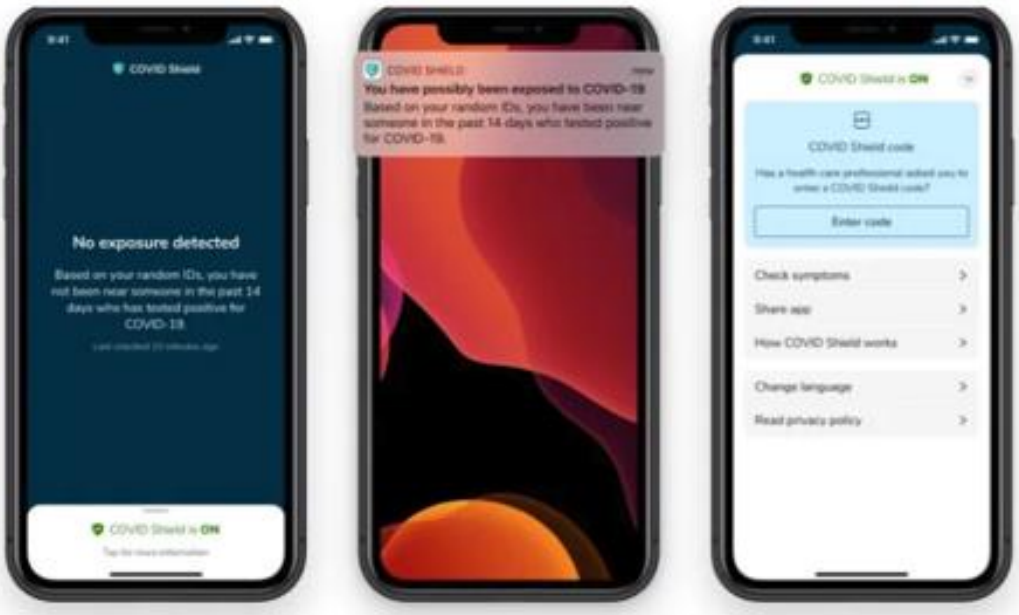
PT UNIVERSAL ADOPTION OF COVID ALERT CANADA IS UNCERTAIN, RISKING PATCHWORK APPROACH

199. Beyond Ontario and Alberta, broader PT adoption of COVID Alert Canada – which would enable its user to report a positive diagnosis – is uncertain, thus risking a patchwork of official apps across Canada.[487] The reason for this uncertainty is that, notwithstanding GoC's expectation that all PTs will adopt the national app at some point: many options for official apps were considered by FPT governments before COVID Alert Canada's endorsement by GoC; as noted, eleven PTs have not yet signed on; and of these, two PTs have publicly confirmed their deliberations are ongoing (PEI and Quebec).

MANY OFFICIAL APP OPTIONS WERE CONSIDERED BY GOVERNMENTS (FPT & MUNICIPAL) BEFORE COVID ALERT CANADA'S ENDORSEMENT

200. **Canadian governments (overall).** Prior to GoC's endorsement of COVID Alert Canada, federal, PT, and municipal governments were reportedly looking at approximately a dozen proposed apps[488] and Health Minister Hajdu said Ottawa's primary decision criterion was privacy safeguards: "We know that privacy is of utmost importance to Canadians and so the work is ongoing right now to look at a variety of different options that has privacy as the first and foremost consideration".[489] According to media reports, "Canadian government officials" were also divided on whether official apps should be mandated or voluntary.[490]

201. **GoC.** At the national level, COVID Shield (see screenshot below[491]) was "arguably the country's most prominent remaining contender"[492] after the federal government rejected another proposed app, Montreal AI research institute Mila's "COVI Canada" ("COVI"), an AI-driven *Bluetooth centralised risk assessment* app (based on the protocols developed by the UK's NHS), due to federal and PT government privacy concerns.[493]



202. **PT governments.** As noted, Alberta (population approx. 4.4M[494]) was the first government in Canada to deploy an official app, ABTraceTogether, on May 1, 2020. This *Bluetooth centralised exposure notification app* was built by Deloitte Canada, using the open-source code for Singapore's TraceTogether, and IBM provides the infrastructure.[495] The province spent approximately $625,000 to develop the app for Canadian use.[496] The app was downloaded 186,000 times in the first 3 weeks (about 4.3% of Alberta's population)[497] and, as of June 18, 2020, had approximately 207,000 registered users (about 4.75%)[498].

203. Other PT governments that signalled plans to adopt their own apps include Quebec, Manitoba, Newfoundland and Labrador, Saskatchewan, and New Brunswick. For example, prior to GoC's rejection of COVI, Quebec's premier was considering partnering with Mila on the app[499]**;** as of June 4, 2020, Mila was still in discussions with the Quebec government, and believed COVI could be made compatible with COVID Shield.[500] Manitoba, Newfoundland and Labrador, and Saskatchewan had plans to "develop" their own apps[501] and New Brunswick ("NB") had decided its app would be built on the Google/Apple API[502]. An unnamed source said several PT governments prefer simpler app solutions than COVI.[503]

204. **Municipal governments.** Some city-level PHAs that were considering their own contact tracing apps paused their efforts (e.g., Ottawa Public Health) after PM Trudeau's announcement of the National Strategy for CTAs.[504]

SOME PTs ARE STILL CONSIDERING OFFICIAL APP OPTIONS

205. Following GoC's endorsement and launch of COVID Alert Canada, some PTs are still considering options for official apps.

206. **Post-endorsement (June 19-July 30, 2020).** After PM Trudeau's endorsement of COVID Alert Canada, on June 19, 2020, following a conference call with the PM and PT premiers, NB Premier Blaine Higgs said plans for the NB app had been thwarted by GoC's choice ("I got clarification that there's one app, and it's a national one") and that the federal government is paying for it.[505] The Manitoba government said it wants to know more about COVID Alert Canada, from a practical and privacy perspective, before signing on, and that "privacy protocols, available advice and legislative obligations will be given proper consideration".[506] ABTraceTogether continued to experience technical problems on both Apple and Android devices and to be beset by user complaints[507], and the Alberta government complained about Apple's refusal to fix the technical issues (however, as noted, this is Apple's standard response to such requests) and that GoC had blocked both tech companies from helping the province fix the problems.[508] On July 9, 2020, the Office of the Information and Privacy Commissioner of Alberta ("Alberta Commissioner") released its report on the app, which praised it for being "mindful of privacy and security" but also made a number of negative findings, including that it could be a "security risk" if used on Apple devices (given "the need to run… in the foreground on Apple devices" which "requires a device to remain unlocked, which significantly increases risk in case of theft or loss").[509] As of July 27, 2020, BC and Newfoundland and Labrador were in discussions with GoC about officially adopting the national app, Quebec had received an app demonstration, and the NB app was "on hold".[510] Quebec's demonstration followed Mila's confirmation, on July 20, 2020, that it had ended its work on COVI.[511]

207. **Post-launch (July 31, 2020 – present).** On August 4, 2020, PEI's chief public health officer, Dr. Heather Morrison, said her province won't make a final decision on adopting COVID Alert Canada until data is available from Ontario to evaluate it.[512] On August 8, 2020, Alberta confirmed that it would not only adopt COVID Alert Canada but also prioritize "seamlessly" transitioning ABTraceTogether's 234,000 registered users (approximately 5.3% of Alberta's population).[513] This goal appears to be inconsistent with the Health Canada Privacy Assessment statement that, "no data from any pre-existing exposure notification/contact tracing apps PTs may already have in place will be transferred to" COVID Alert Canada.[514] On August 13, 2020, a Quebec legislative hearing began devoted to exploring the pros/cons of adopting COVID Alert Canada or a made-in-Quebec app (described by some observers as "technological nationalism"), and the government revealed that around 17,000 Quebecers had engaged in a July 8-August 2 online consultation, with 75% of responses indicating support for a Quebec-specific option.[515] On August 14, 2020, at the end of three days of hearings, the province had still not made its decision, with the three Quebec opposition parties unanimous in their opposition to the national app, on grounds that "(t)he advantages (…) are completely uncertain, but the risks are certain" (e.g., technical, privacy, and security).[516] Previously, Éric Caire, the minister responsible for digital innovation, said that if a Quebec-specific option is chosen, he expects it would be deployed in September 2020; this timeline would likely result in the use of an existing app rather than development of a new one.[517] Also on August 14, 2020, BC Provincial Health Officer Dr.

Bonnie Henry told reporters she is not sure when COVID Alert Canada will launch in the province, while it still undergoes "tweaking" in Ontario, noting BC is still working with GoC "on how we can tailor it to be a tool that supports the work that we're doing in (manual) contact tracing".[518]

208. In light of BC's, Quebec's, and PEI's publicly confirmed ongoing deliberations and the uncertain status of other PT and municipal government plans, there is potential for Canada to end up with a patchwork of official apps, of which some are compatible (e.g., national and PT versions of COVID Alert Canada) and others are not (e.g., COVID Alert Canada and, until it is de-commissioned, ABTraceTogether, since it is centralised[519]). This poses the risk of "confusing messaging, low update numbers, and inconsistent data."[520]

CANADIANS' ADOPTION OF COVID ALERT CANADA (OR OTHER OFFICIAL APPS) IS UNCERTAIN

ADOPTION OF COVID ALERT CANADA: EVOLVING

209. Adoption of COVID Alert Canada has been relatively slow, with 1.1 million downloads as of August 3, 2020, over 1.5 million downloads as of August 7 and 1.9 million downloads (representing 5% of the country's population of 38 million) as of August 13.[521] Downloads can't be divided by geographic location, but an Ontario government spokesperson said it expects the "overwhelming majority" of the downloads would be in the province[522] and, according to media reports, the downloads include "some" Canadians on the East Coast[523]. Alain Belle-Isle, spokesperson for the federal Treasury Board, which is tracking the download rate, said GoC hopes the number of downloads will increase when other PTs officially adopt the app.[524]

210. So far, the download rate is the only measure that is publicly available. The number of active users, number of individuals who have tested positive for COVID-19 and uploaded their diagnosis (if any), number of people who have received exposure notification alerts and, of these, the number that have subsequently chosen to speak to PHAs has not been published. However, GoC "is considering how to track – and potentially make available – data related to the app once other (PTs) adopt it".[525]

211. In other countries, official *Bluetooth decentralized (Google/Apple API)* CTAs provide more data on app implementation. For example, Ireland's "COVID Tracker" counts the number of positive diagnoses recorded in the app and how many users get exposure notifications[526] and Swiss officials regularly post online the number of downloads and active users of "SwissCovid"[527].

WHERE CANADIANS STAND ON DCTT: PRIVACY MATTERS & STATS SHOW CONFLICTING SUPPORT

212. Prior to the launch of COVID Alert Canada, public discourse around DCTT was relatively quiet but mirrored the political debate and focused on the technological aspects of apps. By corollary, it differed from the debate amongst experts, which focused on privacy/security.

213. Pre- and post-launch of the official national app, the position of individual Canadians as consumer-citizens on DCTT is primarily revealed through petitions, survey results, and media reports/interviews. These sources indicate that privacy matters to Canadians (overall) and there is conflicting support for CTAs in general, and COVID Alert Canada in particular.

PETITIONS

214. As of June 19, 2020, nearly 11,000 Canadians had joined OpenMedia's petition to GoC "to commit to key privacy principles" for contact tracing apps, because "clear boundaries are needed to limit the potential harm of such plans to our rights".[528]

SURVEYS

215. **Surveys on privacy (overall).** According to OPCC's 2018-19 Survey of Canadians on Privacy, privacy matters to Canadians: "Individual privacy is not a right we can simply trade away for innovation, efficiency or commercial gain. Canadians agree. An overwhelming majority – 92% – say they are concerned about their privacy, which suggests that having good privacy practices is not just a legal requirement, it is essential to ensuring public trust in our institutions."[529]

216. On May 28, 2020, the Canadian Internet Registration Authority ("CIRA") released a report[530] showing "that Canadians are feeling the need to restore trust online. Right now, many Canadians worry that the dangers online outweigh the benefits – especially when it comes to privacy". In particular, the report found "a significant drop in their willingness to disclose personal information for better content and services online":

> *"In 2019, 72 per cent of Canadians said they were willing to disclose some or a little personal information in exchange for valuable content or service. Only one year later, with the exception of online banking services, the vast majority of Canadians say they are unwilling to share their personal data in exchange for better online services."*

217. **Surveys on CTAs.** Surveys starting in May 2020 show conflicting support by Canadians for contact tracing apps.

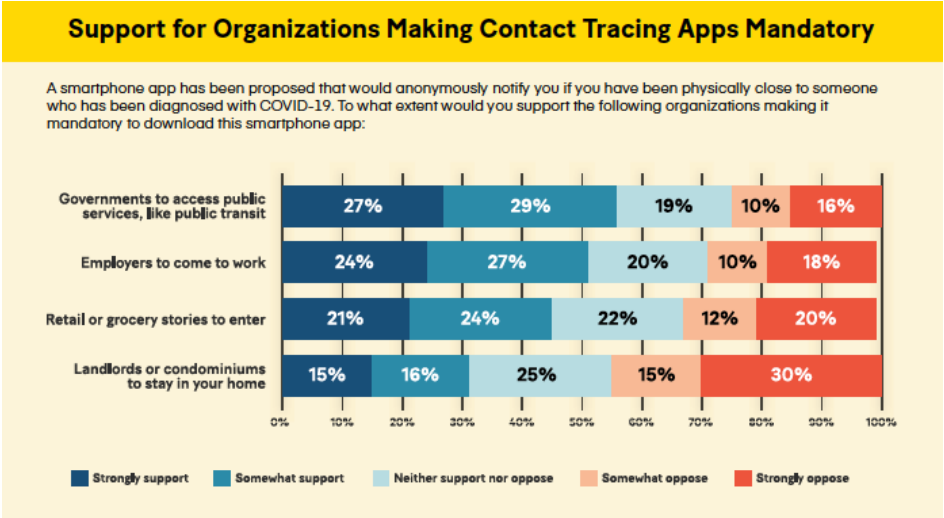
218. In May 2020, three surveys offered conflicting numbers on whether Canadians want contact-tracing apps to be voluntary or mandatory:

- Mainstreet Research survey: a majority of Canadians (57%) would not support a mandatory contact tracing app. All other possible restrictions to stem the spread of COVID-19 received broad support: working from home (79%); mandated mask-wearing at work (80%); mandated temperature-readings before entering workplaces (75.5%); mandated 2 metre distancing at work (83%); and mandated mask-wearing on public transit (76%).[531]
- KPMG Canada survey: 55% of respondents said *digital* contact tracing should be voluntary, citing privacy concerns and potential abuse of civil liberties; 2/3 said they wouldn't download such an app, calling it still "too invasive"; but, 57% don't believe such an app would be effective unless it is mandatory.[532]
- Survey commissioned by three Canadian Senators: 65% of respondents support mandatory use of contact tracing apps.[533] However, one of those senators acknowledged the question on mandatory/voluntary adoption may not have been neutral, and Canadian privacy expert Ann Cavoukian said the Senate survey question "has no validity".[534]

219. A survey conducted by Ryerson University's CPE and reported in June 2020 found that support for a mandated approach varied significantly, depending on the entity in question.[535] Most respondents said certain government institutions (e.g., transit authorities), employers, and retailers should be permitted to mandate contact tracing apps.[536] In particular:

> *"• Majorities [sic] of Canadians supported making contact tracing apps mandatory for the use of public services, like public transit (55%) and in workplaces (51%), though in both cases only one in four Canadians strongly supported such an approach.*
>
> *• Support was somewhat lower (46%) for retail or grocery stores making apps mandatory.*
>
> *• In contrast, opposition to landlords or condominiums making contact tracing apps mandatory (45%) surpassed support (30%).*
>
> *• Between 19% and 25% of Canadians neither supported nor opposed the different scenarios, representing a significant lack of certainty about this approach.*

• Support and opposition for mandatory apps were remarkably consistent across regions, age groups, education levels and gender (see Table 1). There was less consistent support across income […]"[537] *(See also infographic below.)*[538]



220. From PIAC's perspective, the CPE survey reveals that Canadians generally support voluntary apps (i.e., apps whose initial installation and use is not government-mandated) coupled with public and/or private entities mandating mobile device and app or data use (e.g., a clean result) to *access* certain goods, services, and places/spaces. This approach, if implemented, would effectively make voluntary apps mandatory and could exacerbate existing socio-economic inequities:

> *"Requiring access to a mobile device for mobility, employment, education, services or housing has high potential to reinforce and exacerbate existing inequalities. Implicit coercion to use the app, particularly by those in a position of power such as an employer or landlord, will result in unequal treatment and negative consequences for those who cannot, which will likely be already disadvantaged groups."*[539]

Disadvantaged groups include low-income and senior Canadians who do not have a smartphone or lack the necessary data plan to make an app operable.[540]

221. To prevent this situation, contact tracing apps would need to be voluntary and coupled with FPT legislation to prohibit public and private entities from mandating access to the app in order to access goods, services, employment or places/spaces (e.g., workplaces, housing, and parks). This approach has been taken in other countries (see details below), and PIAC supports CPE's recommendation for it to be adopted in Canada (see details in Part <5>).[541] Such action would need to be taken promptly, given that "(s)ome governments, businesses and organizations are considering requiring the use of a contact tracing app for individuals to gain entry to specific locations or to allow employees to come to work"[542] (see details below).

222. On July 24, 2020, the results of an OpenMedia-commissioned Innovative Research Group Poll were reported. The poll says that 29% of Canadians are very likely to download COVID Alert Canada and 41% of people stated privacy concerns were the main reason for lack of confidence in the app. According to a Statistics Canada survey released on July 31, 2020, 56% per cent of Canadians would be "somewhat" or "very likely" to use an app of the same kind as COVID Alert Canada if PHAs recommended it.[543] However, according to an August 2020 Leger Marketing poll, only 20% of Canadians say they will download COVID Alert Canada and potential reasons are that 52% don't believe GoC's claim that the app won't collect their personal data or geolocate them and 39% do not believe the app "will work".[544]

223. On August 14, 2020, iPolitics reported the results of a Mainstreet Research poll that indicates "strong overall support" for COVID Alert Canada, with 70% of Canadians and 77.7% of Quebecers saying they had either installed the app or intend to.[545]

MEDIA REPORTS/INTERVIEWS

224. According to media reports, slow adoption of COVID Alert Canada is due to low trust, stemming primarily from "deep-seated doubts" about effectiveness and privacy, notwithstanding "(t)he federal government, digital privacy advocates and software experts have provided assurances that (the app) is safe".[546] For example, some Canadians on the East Coast have not downloaded the app because they "remain apprehensive and unconvinced due to privacy worries…anxious about the app being, or eventually becoming, a Big Brother that tracks their every move".[547]

IDENTIFYING KEY FEATURES OF OFFICIAL APPS, THEIR INTER-RELATIONSHIP & RELATIONSHIP TO OTHER DATA-DRIVEN GOVERNMENT RESPONSES TO COVID-19 IS ESSENTIAL FOR COMPREHENSIVE PRIVACY ANALYSIS

225. Identifying the privacy-related features of all of Canada's official contact tracing apps – including but not limited to COVID Alert Canada and PT-customized versions such as COVID Alert Ontario – as well as their inter-relationship with each other and with other FPT government data-driven responses to COVID-19 (manual and digital), is essential to conduct a comprehensive privacy analysis.

226. However, the rest of this document focuses on COVID Alert Canada and COVID Alert Ontario.

PIAC'S ANALYTICAL RUBRIC FOR APPS IS AN IMPORTANT TOOL

227. To facilitate PIAC's comprehensive privacy analysis of official contact tracing apps (current and future), we created the following analytical rubric ("PIAC Analytical Rubric for Contact Tracing Apps") (see Table). Contact tracing apps can be described in terms of multitudinous features. For ease of reference and understanding, PIAC believes these features are best identified at two levels, app and data.

Contact Tracing App	
App type & OS	Voluntary/mandated? Location/proximity-based? Centralised*/decentralised? Notification exposure/risk assessment/tracking? Based on what API? For what OS (Android and/or iPhone) and requirements (Android 6.0 or higher? Apple iOS 10 or higher and iPhone 5S model or higher)?
App status	Government endorsed/sanctioned: endorsed ("official") or not endorsed ("unofficial")? Deployment: Deployed? Available where (e.g., App Store [iOS] or Google Play Store [Android])? Free or fee? Adoption rate (e.g., high or low)?
App developer & infrastructure provider	Developer: Government, private organization (business or other), public-private partnership? Infrastructure provider: Whose *servers (e.g., Amazon Web Services)? Located where (e.g., Canada or other country?
App details	How it works (overall): Self-reporting of infection? Without or with verification by registered health care provider or PHA ("presumed case" or "confirmed case")? What are the key steps? Interoperability: Does it work in one PT only? Does it connect to other contact tracing apps? User control: Login/logoff at own direction ("yes") or once installed can only be stopped by turning off location/Bluetooth ("no")? Requested permissions: Potentially intrusive (e.g., access camera or read contacts)? If yes, used for legitimate purpose(s) (e.g., so users can share app with friends)?

	Technical issues: Battery affected? Only functions when app is in use ("open") or running in foreground?
Contact Tracing Data	
Data collection	Collection[548]: Only from infected users (presumed or confirmed)? When - at app sign on/registration only or ongoing)? What/nature - only about user or also about third parties? Personal and if yes, what type(s) (e.g., health)? How much/volume – only what is "necessary" (i.e., needed to carry out app's legitimate purpose[s] [see below], or more)? Collector(s): Government institutions (PHAs [ideally] or other [e.g., law enforcement])? Private organization (business or other)? Public-private partnership? (Note: users require *access*, thus are also "sharers") Collection purpose: Specific? Limited? One purpose (public health in general or, specifically, effective contact tracing or infection control (see app type)? Secondary purpose(s) (e.g., epidemiology, research, data analytics, app performance)?
Data use[549]	Use(s): What use(s)? Only what it necessary to fulfil the purpose (see below)? Used how (de-identified [anonymised or pseudonymized], disaggregated, derived/inferred, combined with data from other sources ["linked" or "matched"[550]]), with what tools (e.g., AI)? User(s): Government institutions (PHAs or other)? Private organization (business or other)? Public-private partnership? Use purpose: Specific? Limited to purpose(s) for which it was *collected* (if not, "risk of function creep"[551])?
Data disclosure[552]	Disclosure: What data (e.g., *Infected user's identity* or other identifying data)? Only what is necessary to fulfil the purpose (see below)? Sharer(s): Data shared by primary user with third parties ("sharers") (e.g., other app users, government institutions [PHAs or other], private organizations [business or other], public-private partnership)? Within or outside PT ("extra-provincial disclosure") or Canada ("international disclosure")? Free or fee? Pursuant to contract with privacy provisions that bind sharers to user's own privacy protections? Disclosure purpose: Specific? Limited to purpose(s) for which it was *collected*?
Data retention[553]	Storage location: Centralised server or local (user's device)? If centralised, is *infected user's identity* stored? Storage time: How long is data kept (indefinite or time limited)? What time period (only as long as epidemiologically useful for contact tracing, that is, period virus is contagious plus reasonable time for testing and notification, which based on current evidence is maximum 30 days[554])? Storage purpose: Specific? Limited to purpose(s) for which it was *collected*? Deletion: *Data* deleted, from device or server, after appropriate storage time (see above)? Automatically or by user, in-app? Permanently? Can user otherwise stop sharing data (e.g., withdraw consent at any time)? *App* deleted or disabled when pandemic ends or adequately contained ("sunset point")? How is sunset point determined (e.g., connected to rate of community spread or vaccine deployment)?
Data security[555]	Expressly addressed? Data encrypted? Other physical, technical, or administrative protections?
Transparency, notice[556] **& consent**	Source code: Publicly available ("open source") or proprietary? Notice: Timely, context-specific notifications for individuals re: data practices and choices ("notifications")[557], for consent or other purposes? Basic description of data practices aimed at general audience of individuals ("privacy policy/statement" and if yes, app-specific ("app-specific privacy policy") or organisational ("general privacy policy")? Publicly available (e.g., website, app store)? Privacy policy violated by app's own data practices? Consent: (Informed) consent required to collect, use, and disclose personal data? For each and every purpose? Explicit/implicit[558]? Affirmative ("opt-in") or opt-out? Obtained when (e.g., at time of signing up/registering for app, prior to or at point of data collection, or periodically renewed)? (see details above) Clear limits: On data collection, use, disclosure, etc. (see details above)?

	Oversight: PIA conducted (internally) and if yes, submitted for review by privacy commissioner(s)? Independent assessment of app by privacy commissioners (via PIA or complaint), before or after deployment? Ongoing oversight of app's effectiveness alongside manual contact tracing (to determine whether risks to privacy outweighed by benefits to public health)?
Other Considerations	
App or data use mandated (by public or private entities) *to access* goods, services, employment, workplaces, housing, or other spaces/places	App or data use (e.g., clean result) mandated – by public or private entities – *to access* goods, services, employment, and places/spaces (e.g., workplaces, housing, parks)?
Privacy commissioner(s)' review/comments	Received PIA (see above) and, if yes, what is status? Received complaint and, if yes, what is status? Issued comments or decision? If yes, supportive or opposed?

COVID ALERT CANADA & ONTARIO: KEY FEATURES

228. As noted, COVID Alert Canada and COVID Alert Ontario are distinct. However, as of July 30, 2020, the day prior to the launch of COVID Alert Ontario, few details about either app had been officially announced, and available details lacked clarity.

229. This paucity of official information was alleviated, to some degree, with the launch of COVID Alert Canada and Ontario on July 31, 2020, and the same-day pronouncement by OPCC and the Ontario Privacy Commissioner that the app meets all of the key federal and Ontario privacy principles based on their respective privacy assessments. However, certain details remain uncertain due to lack of transparency, including the absence of an official comprehensive "data flow analysis", defined as a diagram and table that describe the purpose(s) and legal authority for each "information flow" (i.e., each collection, use and disclosure of personal information).[559] A data flow analysis is a common element of PIAs[560] and it is essential for a thorough analysis of a given app's privacy risks and reasonable measures (administrative, technical, or physical) to mitigate them. This is especially true for PT versions of COVID Alert Canada, which by definition have PT-specific data flow elements due to PT-specific public health systems.

230. The rest of this section provides, based on publicly available information, a description of: COVID Alert Canada and COVID Alert Ontario (using the PIAC Analytical Rubric for Contact Tracing); their inter-relationship; and their relationship with other DCTT and broader data-driven (manual and digital) government responses to COVID-19.

COVID ALERT CANADA

231. According to some experts, COVID Alert Canada "(i)n many ways… benefitted from watching others launch and is fortunate to be focusing on such manageable challenges around public trust in technology deployment".[561] PIAC believes that whether the app has *successfully managed* these challenges, specifically privacy challenges, is the fundamental question for FPT privacy commissioners, privacy experts, and public interest advocates. We also ask this question in our separate CRTC Part 1 Application regarding telecommunications law.

APP

232. **Type.** COVID Alert Canada is a *voluntary Bluetooth decentralised (Google/Apple API) exposure notification* CTA that is free of charge to download on Apple and Android smartphones from the Apple and Google Play app stores.

233. The Ontario government news release on the launch of COVID Alert[562] ("Ontario government news release") emphasizes that "all aspects" of the app "are completely voluntary", specifically: "whether to download the app, whether to use (it)… and whether to notify others if they test positive for COVID-19".

234. "During the technical briefing, federal officials emphasized that it should not be considered a contact tracing app, though it has previously been described as such by federal and provincial politicians".[563] This distinction is also reflected in the privacy assessments of Health Canada and the Canadian and Ontario Privacy Commissioners. This purported distinction between "contact tracing" and "exposure notification" apps is inaccurate, given the latter are, in fact, a subset of the former. PIAC believes this inaccuracy could be well-intentioned, to prevent confusion with contact *tracking* apps (supported by Health Canada's equation of "contact tracing apps" with apps "collecting geolocation data and reporting this to [PHAs]"[564], i.e., location tracking). However, regardless of intent, we believe that terminological accuracy and consistency is important to ensure that COVID Alert Canada and broader DCTT can be discussed in a transparent way that advances the ongoing policy debate about their use.

235. **Developer(s) and owner(s).** According to the June 2020 PM Trudeau announcement, GoC is "leading the development of the app", which was "originally developed by the Government of Ontario"[565], and the "technology will be owned and operated by the Government of Canada, and published under an open source licence".[566] The Ontario government news release on COVID Alert Canada's launch[567] refers to COVID Alert Canada as a "made-in-Ontario" app "initiated in Ontario by (ODS) and volunteers at Shopify" and developed by GoC "in consultation with the Privacy Commissioners of Canada and Ontario". In a series of post-launch tweets, CDS CEO Aaron Snow said: "(t)his product took 45 days to launch, with 3 product teams working in tandem… three security review teams, from the Canadian Centre for CyberSecurity, the office of the CIO, and an audit team from Blackberry".[568]

236. Shopify (TSX:SHOP) is an e-commerce company that provides clients with cloud-based SaaS (software as a service) solutions for online commerce, allowing merchants to operate online businesses selling a wide variety of physical and digital products, as well as services.[569] Clients pay a monthly fee to enjoy access to a dashboard app on which they can design their online storefront, process orders, ship products, view business analytics, and create detailed customer profiles.[570] The merchant's Shopify app can run on computers as well as iPhone or Android smartphones and tablets, allowing merchants to manage retail operations from mobile devices.[571] Both the merchant's online stores and inventory are hosted on Shopify's servers.[572]

237. Since its founding in 2004, the company has integrated its services and platform with numerous other companies, including Amazon[573], Facebook, Google and Snapchat.[574] While Shopify is not historically involved in the public health sector, many entrepreneurs use Shopify to operate their businesses in the health and wellness market.[575]

238. As noted, according to the Ontario government, Shopify's work with ODS was provided on a *volunteer* (i.e., unpaid) basis. According to a Treasury Board Secretariat (TBS) spokesperson, as of July 27, 2020, a "handful" of Shopify developers remain "heavily involved" with the project as part of the Interchange Canada program (which allows secondments between the federal public service and industry) and are being paid by the government.[576]

239. BlackBerry Ltd. (TSX:BB) sells products (e.g., smartphones) and enterprise software and services, including: Enterprise Solutions and Services, Devices, BlackBerry Technology Solutions and Messaging. BlackBerry once controlled 20% of the mobile phone market at its peak in 2011, but the company has since shifted its focus from hardware to cybersecurity, crisis communications and embedded software.[577] The majority of

BlackBerry's current revenue is earned within three categories of products and services: security software, Internet-of-Things (IoT) solutions, and IP licensing.[578]

240. BlackBerry's involvement within the health sector is extensive. BlackBerry provides numerous software solutions that support patient data storage, medical devices, and emergency notifications in the healthcare industry.[579] BlackBerry is also well-positioned to play a large role in developing IoT infrastructure in the health sector as more devices are connected to the Internet and each other. Much like its consulting role with COVID Alert Canada, BlackBerry provides consulting services to help address digital infrastructure needs of healthcare organizations around the world. Blackberry's cybersecurity expertise is increasingly utilized as healthcare becomes increasingly digital through connected hospitals, wearable devices and implants, and advanced medical research.[580] In 2020, Blackberry proposed using artificial intelligence technology to make hospital operations more adaptive and autonomous.[581]

241. According to Blackberry CTO Charles Eagan, the company *volunteered* to perform auditing and stress-testing for COVID Shield Canada and a number of other proposed official apps, including Mila's COVI.[582] Eagan said "implementing security that is comprehensive and protects against both external attacks and inadvertent breaches" in COVID Alert Canada is vital because: "Without this level of security (…) there is no hope of privacy. And without privacy, there is no hope of mass adoption."[583]

242. PIAC notes that in other countries, "volunteer" work by businesses on or related to official apps has potentially significant benefits for those businesses in terms of future paid government contracts (e.g., above-noted UK NHS-Palantir data initiative).

243. **National v. PT version(s).** The app's functionality appears to be effectively divided into two parts: part 1 (national app) is standardized, for use during the exposure notification period, whereas part 2 (PT version) is customized, for use if/when a user tests positive (see details below under "data flow"). The Health Canada Privacy Assessment:

- describes the "single, national app" having "three elements" (mobile app [federal level], key server [federal level], and one-time code distribution process [PT level]);
- confirms that "(w)hile the user experience may differ by PT, the data flow will not"; and
- highlights a *possible future functionality* that has been added by other countries, specifically "a voluntary flow to allow notified users to upload these notifications for public health analytics purposes, a function that is compliant with the terms of" the Google/Apple API, and undertakes that "If such functionality were being considered (and note it is not at present), we would re-engage with" OPCC.[584] The OPCC privacy assessment acknowledges the possibility of new uses or disclosures of data (e.g., adding anonymous diagnostic data to help measure the app's adoption), but emphasizes it would be only with consent.[585]

244. **Technical (device specs).** The GoC Accessibility Statement for COVID Alert Canada[586] says it "works across the range of phones supported by Google and Apple exposure notification technology, as long as the phone has at least an Android 6 or Apple iOS 13.5 operating system". This means an "Apple or Android phone released within the past 5 years" (according to CDS) and excludes models older than the iPhone 6S (according to media reports).[587] As of August 7, 2020, according to Digital Government Minister Murray, "(t)his is a Google-Apple foundational API issue" and GoC has "asked them to explore how they could address that. It's in Apple and Google's hands".[588]

245. The GoC Accessibility Statement recognizes that "(s)ome people may have phones or operating systems that do not support downloading the app", "may not have smart phones at all" or "may not have affordable access to the Internet" (noting "the app needs an Internet connection at least once a day to work"). However, it proceeds to assert these people "can still benefit from it, if other people use it" (e.g., a notified user could decide to not visit a medically vulnerable person without a smartphone, which protects that person from potential exposure). It is generally recognized that *smartphone ownership and quality* tends to be lower among Canadians who are especially vulnerable to the virus (e.g., older, lower-income, and racialized people).[589] Chief Public Health Officer Theresa Tam acknowledged these "gaps" but contends

that: COVID Alert Canada is not intended to be a comprehensive solution; "extremely relevant" targets are younger people with newer phones and office workers with employer-issued devices; and manual contact tracing will be used for "the hard-to-reach populations".[590] This message was echoed by Minister Murray.[591] A spokesperson for the president of the Ontario treasury board, in an emailed statement, said an estimated 90% of Ontarians have access to a smartphone and the "vast majority" are able to download the app, however no specific number is available.[592]

246. In addition to device specifications for running COVID Alert Canada, as noted, global concerns have been raised about data collected by Android devices pursuant to the Android location requirement. At the time of the launch, Canadian "officials" acknowledged the Android location requirement pertains to Android devices on which COVID Alert Canada is installed but downplayed concerns on grounds the app will not know a user's location, name, or address.[593] Google says a fix is coming in fall 2020 (see details below).[594]

247. **How it works (overall).** According to PM Trudeau and the Prime Minister's Office ("PMO") on June 18, 2020:

- "If you test positive for COVID-19, a health care professional will help you upload your status anonymously to a *national network*. Other users who have the app and have been in proximity to you will then be alerted that they've been exposed to someone who's tested positive".[595]
- PHAs will "distribute the unique, temporary codes to people who test positive".[596]
- "There will be a *database* of randomized codes associated with each smartphone that has this app that will be divided into two columns, those who may have tested positive and those who have not tested positive".[597]
- "So if your phone gets in proximity for a certain amount of time and a certain closeness to another phone, it will register it has had contact with that anonymized…identifier for the app."[598]

248. Prior to the launch of COVID Alert Ontario, media reports said "the app's interface would be managed by the participating province"[599] but, in order to have a standard privacy and security perimeter for Canada[600], "the Canadian Digital Service will control the 'secure' national database that will hold all the randomized codes"[601] (aka "will host a *secure universal key server* as a *central depository* for all the *anonymous proximity data* generated by the app's users"[602]).

249. The foregoing details were clarified with the launch of COVID Alert Canada. The proximity data specifically pertains to Bluetooth signal strength between phones that are running the COVID Alert Canada app. The COVID Alert Canada launch page states that "(w)henever you're near someone else with COVID Alert, both phones exchange random codes every 5 minutes," and these random codes cannot be used to identify users.[603] The app only records exposures when signal strength corresponds to a proximity of closer than 2 metres for more than 15 minutes.[604] The Health Canada Privacy Assessment assures that "(t)his Bluetooth communication between participating users is short-range device-to-device communication; nothing is transmitted to any server."[605]

250. For the Bluetooth exchange to work, Android phone users have to turn on the general Location setting for all apps, which gives Google and other apps access to users' location even though the COVID Alert Canada app itself does not have permission to use the phone's location services.[606] However, Google is set to remove this requirement in the next update, Android 11, expected to release on September 8, 2020.[607]

251. The user's random codes from the last 14 days are uploaded to the central key server only when a user submits a one-time code provided by a PT PHA who has also adopted the app.[608] These one-time codes expire after 24 hours have passed since the PT PHA gave them out, "to give people time to process, and make an informed decision, when they were ready."[609] With daily access to the Internet, each user downloads new diagnosis keys from the server when the app is opened and once every 4 to 24 hours depending on the phone's battery level and frequency of Internet access.[610] Within the phone, the app collects data on the date, duration and signal strength associated with the random codes, but this information is never sent to the server.[611]

252. **Server**. On July 2, 2020, an unnamed Ontario government official who was not authorized to speak publicly said the COVID Alert "launch date was delayed because the federal government wanted the app to launch… *with a federal server for the app rather than a provincial server* and internal processes and approvals on the federal side required additional time".[612]

253. Server details were clarified with the launch of COVID Alert Canada. Users can view how many keys their phone has downloaded from the federal key server by accessing the COVID-19 exposure notifications page in their phone settings.[613] In the "Exposure Checks" logs, the number indicated under "Provided Key Count" for Apple users (in the beta version, now named, identical to Android, "Number of Keys") or "Number of keys" for Android users is the "number of keys related to a positive test result, so called diagnosis keys, that your phone downloaded from the server."[614] The number under "Matched Key Count" (Apple) (in the beta version, now named, identical to Android, "Number of Matches") or "Number of matches" (Android) pertains to "the number of keys that your phone collected for which there is a matching diagnosis key."[615]

254. The server codes are "retrieved by other people's phones with the app installed, to alert them that they were in contact with someone who was COVID-positive."[616] The exposure notification does not reveal the identity of those who tested positive, but OPCC said that "[s]omeone living in a remote area and only interacting with one or two people could theoretically be identified by their neighbours if they received exposure notification alerts, for example."[617]

255. In OPCC's review of the Health Canada Privacy Assessment, it concluded that "(a) thorough evaluation of the surrounding technical ecosystem in which the app operates is beyond the reach of this review," as the Google/Apple API code is not entirely publicly available.[618] OPCC, in light of the limited time it had to review the assessment, reserved the right to further review the agreement under which GoC procured the AWS server (see details below).

256. **App deletion ("decommissioning").** Health Canada has made the commitment to shut down the app as a whole within 30 days of a declaration by the Chief Public Health Officer of Canada that the pandemic is over, the criteria for which has yet to be determined.[619] The post-pandemic shutdown will erase the key server, the one-time code portals, as well as the download link on the Apple and Google app stores. On August 7, 2020, Minister Murray said the app can be quickly decommissioned and she will take guidance from the Advisory Council on when it is no longer needed and should be sunsetted.[620]

257. **Oversight.** At the time of the June 2020 PM Trudeau announcement, the PM and PMO said GoC "will establish an external advisory council that includes regional representation, to provide guidance during the roll-out of the app with a view to ensuring it operates in a transparent way and in the public interest".[621] On July 31, 2020, GoC announced the launch of the "COVID-19 Exposure Notification App Advisory Council" to "ensure the app meets the highest standards in public health outcomes, technology, and privacy".[622] Council members include Dr. Brenda McPhail, Director, Canadian Civil Liberties Association's ("CCLA") Privacy, Surveillance and Technology Project. The advisory council's Terms of Reference provides for potential "consultations with external stakeholders from industry, civil society and academia, as well as observers to incorporate broader Canadian perspectives into fulfilling their Program of Work."[623]

258. During the roll-out of the app, GoC committed to involving OPCC "in an audit of the app after it is up and running, though no official details have been announced," and this audit will include "an ongoing evaluation of the app's effectiveness and security measures."[624] Planned to begin in the fourth quarter of 2020, the audit will "include as part of its mandate the ongoing analysis of the necessity and proportionality based on a framework and benchmarks being developed by Health Canada with the advice of the public health epidemiology experts."[625] Some level of public oversight is also possible due to the app's code and real-time software developments hosted on Github, where anyone may monitor ongoing app developments and issues.[626]

259. **Security vulnerability reporting.** App users who find a security vulnerability can notify GoC by submitting an anonymous report.

DATA

260. **Location services and personal data (overall)**. At the time of the June 2020 PM Trudeau announcement, the PM and PMO said:

- "At no time will personal information be collected or shared and no location services will be used".[627]
- "(T)he app will not disclose the identity of users. This information will never be shared with any other entity, will not be stored by the app, and will never leave the user's phone. No personal information is collected by the app, and it does not track the user's location".[628]
- "Because it's completely anonymous, because it's low maintenance, because it is completely respectful of your privacy, also including no location services or geo-tagging of any sort, people can be confident that this is an easy measure that they can have to continue to keep us all safe".[629]

261. When COVID Alert Canada was launched on July 31, 2020, PM Trudeau reiterated in his press briefing, "it doesn't collect your name, your address, your geolocation, or any other personal information."[630] On launch day, the Ontario government, in its news release, stated, "(t)he app does not collect personal information or health data, and does not know or track the location, name, address, or contacts of any user," further claiming that the app "was built using the Apple/Google framework for exposure notification to ensure it leverages global best practices to protect privacy".[631] GoC released a promotional video upon launch that assures, "no one will know who you are or where you have been."[632]

262. PIAC notes the Health Canada Privacy Assessment refers to "personal information" interchangeably with "personally identifiable information" and "PII".[633]

263. **Data deletion**. Prior to the COVID Alert Canada test phase, the Ontario government said COVID Alert Canada "automatically destroys all anonymized data" it contains after 14 days.[634]

264. In the officially launched app, the privacy policy accessible through the app's splash page states that all random codes are deleted from the user's phone and on other phones after 15 days.[635] After the user deletes the app, the codes on the user's phone, as well as any codes uploaded to the server, are automatically deleted after 15 days. The user can also delete the random codes on their phone at any time by manually going into the "COVID-19 exposure notifications" settings and deleting the exposure logs or random IDs.[636]

265. As noted, Health Canada has committed to shut down the app as a whole within 30 days of a declaration by the Chief Public Health Officer of Canada that the pandemic is over. As for aggregate, anonymous data, Health Canada states only that "retention of the data will be assessed to ensure it meets all requirements."[637]

266. **IP Addresses.** The users' uploaded diagnosis keys are encrypted and stored on GoC's key server, operated by CDS and located in Canada. This server is operated on a cloud solution provided by AWS and procured through the Government of Canada Cloud Brokering Service.[638] Although only the diagnosis keys are stored on the federal key server, users' IP addresses are also potentially associated with requests made to the key server. IP addresses are retained for sixty minutes in the key server only when the user attempts to input an invalid one-time code. The IP address is deleted from the key server sixty minutes after the last invalid attempt, and is blocked for sixty minutes after eight consecutive invalid attempts from the same IP address.[639]

267. The IP addresses accompanying all requests to the key server are stored separately within access logs on an AWS server. The access logs are retained in the AWS server for 3 months, and up to 24 months if implicated in a cybersecurity investigation "to adequately understand, monitor, and respond to attacks against a system and for the secure and reliable operation of the service."[640] With regard to these retention periods, a developer at CDS stated, "(l)ess than 3 months is not expected to provide sufficient data to perform these actions," that is, "to properly investigate and action any security breaches."[641] The possibility still stands

that the retention period may decrease as CDS better understands how the system operates in real-life scenarios.[642]

268. CDS has committed to not using the IP addresses to identify the source, but the "IP addresses may be disclosed to law enforcement in the event a malicious actor attempted to gain, or gained, access to the server where they are stored."[643] The AWS server will continue to operate after the end of the pandemic, but the IP addresses will be deleted along with the codes on the key server, unless retained for any security investigations.[644]

269. OPCC acknowledges that, although the risk is low, the retention of IP addresses in access logs "present a risk of re-identification because, when combined with other information, IP addresses can be used to identify individuals."[645]

270. **Data Access**. Health Canada's privacy assessment claimed that "Google/Apple will not have access to the data" on the app, neither will any other app on the phone.[646] Health Canada states that CDS also cannot access both IP addresses and subscriber lists of ISPs to connect any IP address to an individual.[647] When external support is employed to review the code and infrastructure of the app, these external parties will not have any access to the system data. If external developers are engaged, they will be contractually subject to the same standards, and security clearances where necessary for sensitive data, as those employed by GoC.[648]

271. **Data flow.** Based on what Health Canada has disclosed about how the app operates, there are four major entities or loci that handle data: GoC, PTs, the user's mobile device, and the AWS server that stores IP addresses. There are four main types of data that individually flow between the entities: Rolling Proximity Identifiers (RPIs), diagnosis keys, one-time codes, and IP addresses (see infographic).

272. RPIs, which are random IDs generated from temporary exposure keys, are generated and shared only between users' mobile devices that have the COVID Alert Canada app activated.[649] The Government of Canada generates one-time codes, then provides them to the PTs, who in turn provide the codes to users who test positive.[650] Health Canada explicitly states that the PTs delete the one-time codes once they are passed onto users, but it is unclear whether GoC also deletes the codes.[651] The code is not retained in the user's app after the user submits the one-time code to the central key server.

273. Once the one-time codes are validated by the key server, the user's diagnosis keys are uploaded to and stored on the central key server controlled by GoC and operated by CDS.[652] On a daily basis, the user's app downloads the updated list of diagnosis keys from the central server. It is not clear from the privacy assessment what the line is between CDS and the Government of Canada. The assessment, on multiple occasions, emphasizes how CDS' control of and access to data is limited, but does not delineate similar limitations on GoC.

274. With each transmission request to the central key server, the user's IP address is also collected as metadata, and stored within a separate AWS server. It is unclear based on Health Canada's privacy assessment whether IP addresses first go to the Government of Canada's key server, then are passed onto the separate AWS server.

275. None of the data within the continuum of the app's operations are accessible by Google/Apple, Shopify, or BlackBerry (see details below). As noted, currently, the data are not used for public health analytics, but should that become a possibility in the future, GoC will re-engage with OPCC.[653]

276. For a schematic of data flows in COVID Alert, please see Figure 1, below.

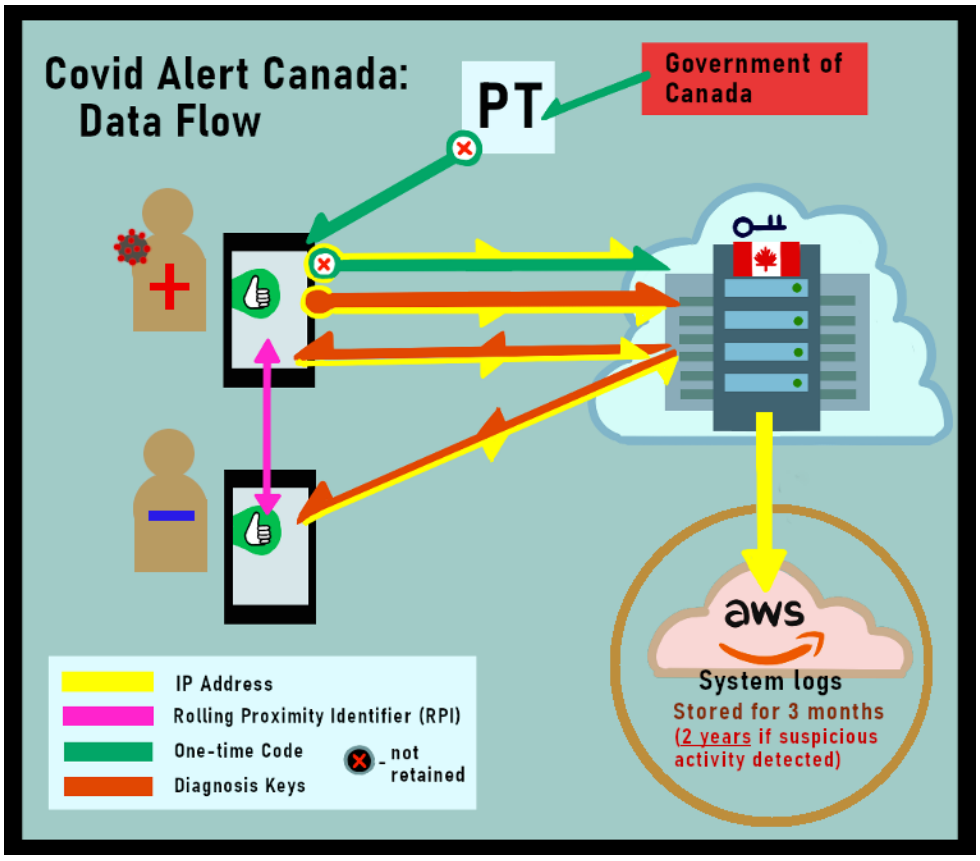


Figure 1: How IP addresses are associated with diagnosis codes under COVID Alert
Source: PIAC

277. **"Partners and stakeholders"**. The Health Canada Privacy Assessment identifies the following "partners and stakeholders" in COVID Alert Canada, both government and business, and their respective roles/responsibilities[654]:

Partner/Stakeholder	Role
Health Canada ("HC")	Overall app implementation, PT engagement, and privacy assessment (including "engaging" OPCC for "meaningful consultation and feedback"
Treasury Board Secretariat – CDS	Develops app, operates GoC key server, provides IT services to HC, and supports PTs to "integrate one-time code distribution into their result notification processes"
Industry, Science and Economic Development ("ISED")	Develops, implements, and supports "governance model to support the effective roll-out of the app"
Canadian Centre for Cyber Security (CCCS/Cyber Centre)	Provides expert cyber security help but not involved in app's operation and does not collect or analyze user information in connection with app
Google/Apple	Developed Google/Apple API and will not have access to app data

Shopify	Volunteers developed "open source software code compatible with the Google/Apple API" used by GoC Neither Shopify nor individual volunteers can add any code to app and "(a)ny staff who may be brought into the CDS team to support will be managed in accordance with Treasury Board staffing policies"
Blackberry	Reviewed security of source code "on a pro bono basis" and "(a)t no point will … have or require any access to data"
External support ("hands-on capacity")	These individuals will be "under contract (either through procurement or through mechanisms like Interchange)" to "ensure they are held to the same standards" as GoC direct employees.

COVID ALERT ONTARIO

278. **Since COVID Alert Ontario is a customized version of COVID Alert Canada, this section identifies customized features only.**

APP

279. **Ontario v. national app.** Prior to the COVID Alert Canada beta test phase, the Ontario government said that COVID Alert Canada would be customized to "provide users with quick access to Ontario's public health advice and resources, and recommend any necessary actions, such as monitoring for symptoms, self-isolation or appropriate next steps on getting tested"[655] (i.e., *information provision +* exposure notification app).

280. **How it works (overall).** The information available prior to the COVID Alert Canada test phase regarding the basic functionality of COVID Alert Canada, described above, indicates that CDS controls the "national database" and that PTs (hence, Ontario) "manage" the "app interface".

281. As noted, although the launched app is available to download across all PTs, only Ontario's health system, as of August 15, 2020, is issuing the one-time codes required to report positive diagnoses on the app.[656] To generate the one-time codes that users input upon positive diagnosis, PT healthcare providers have two options: they can "connect their healthcare IT systems directly to the server software via API, to generate one-time keys automatically," or use a separate but optional healthcare portal for generating unique one-time codes for COVID-positive patients.[657] The underlying code and continuing development for the latter is accessible to the public on CDS' Github repository.[658]

282. In Ontario, patients who test positive can access and view their COVID-19 test results from a web-based tool that collects laboratory test information from participating labs across Ontario. COVID-positive patients can use the website to request a one-time key for the COVID Alert app. The website's Terms of Use states that the patients' "personal information or personal health information is not provided by the Ministry – or by you – to Health Canada or to the App."[659]

283. The purpose of exposure notifications, as stated in the Health Canada Privacy Assessment, is to allow users "to identify whether they have been exposed to the virus and thus take appropriate steps to further reduce the spread."[660] Exposed users will receive a message that "lets them know that they are at risk of being infected and prompts them to contact their local public health agency to determine next steps." [661] If the user has received an exposure notification, the app will supply information stored in the application, such as testing locations.[662] On the exposure notification screen, the user can click on "Find out what to do next" to be directed to an external website for public health advice.[663] In Ontario, users who get an exposure notification alert "should follow the public health advice given on the app and get tested".[664]

284. **Server**. As noted, according to an unnamed Ontario government official, the COVID Alert Ontario launch date was delayed because GoC wanted a federal rather than provincial server. Prior to the launch of COVID Alert Ontario, Matteo Guinci, strategic communications and media advisor from Ontario's Ministry of Government and Consumer Services, said the app does not send "any data to any Government of Ontario server". Rather:

> *"In order to ensure that a positive diagnosis is legitimate, people will access the Ontario COVID-19 lab results viewer – an online method of receiving one's test result to retrieve a unique code that the individual will enter into the app voluntarily to notify others of exposure. The lab results viewer is not a part of, or connected to, the COVID Alert app".*[665]

DATA

285. **Data Security**. Health Canada acknowledges that the risk of identification arises at the provincial level where "someone with direct, server/database-level access to PT healthcare systems (healthcare worker, an IT person, or a malicious actor who'd broken into those systems) could determine whether or not a specific person who received a positive diagnosis had then decided to upload diagnosis keys."[666] As such, the "PTs will be expected to use sufficiently strong cryptographic hashing algorithms (implementing appropriate security measure will form part of the agreements with the provinces)."[667] According to the OPCC privacy assessment, the GoC-Ontario government Memorandum of Understanding ("MOU") on COVID Alert "includes rigorous privacy clauses".[668]

COVID ALERT CANADA RELATIONSHIP TO OTHER DATA-DRIVEN FPT GOVERNMENT RESPONSES TO COVID-19 IS TANGLED & UNCERTAIN

286. There is "an increasing desire across Canada for more data on COVID-19 to be collected as well as shared"[669] and FPT governments are responding. In addition to official CTAs COVID Alert Canada/Ontario (and future PT versions thereof), data-related FPT government responses to COVID-19 pertain to:

- Other DCTT (CTA and non-CTA), official and unofficial;
- Broader digital "outbreak response" and health technology; and
- Enhanced manual contact tracing.

The relationship between these data-gathering initiatives and COVID Alert Canada/Ontario (and future PT versions) is typically unspecified and therefore uncertain. This uncertainty makes it impossible for Canadians to accurately identify data flows within and between PTs and other countries, which has significant privacy implications.

COVID ALERT CANADA RELATIONSHIP TO OTHER DCTT (OFFICIAL & UNOFFICIAL)

287. **Relationship to other official DCTT (present/future).** COVID Alert Canada co-exists with other *official* national CTAs, such as the CBSA's ArriveCAN contact tracing app for use by out-of-country travellers arriving in Canada[670] (noting the Canada-US border remains closed to non-essential travel until at least September 21, 2020[671]). ArriveCAN enables travellers to submit their information to GoC before arriving in Canada, including "mandatory information that's required for entry into Canada" and "voluntary updates on your quarantine compliance and the development of any symptoms during the 14 days after arriving in Canada".[672] On July 29, 2020, certain Conservative MPs issued a press release saying they had written to OPCC asking it to investigate ArriveCAN and providing a link to their letter of the same date.[673] According to the letter, the app contains a provision that states: "personal information may be disclosed to the following entities: law enforcement (including, in particular, peace officers), other government institutions, as well as provincial, territorial, municipal governments or organizations as well as their institutions for these purposes" and "(i)n limited and specific circumstances, personal information may be used and disclosed

without consent in accordance with subsection 8(2) of the Privacy Act". On July 31, 2020, an OPCC spokesperson said that PHAC "consulted with our office in June on border screening activities related to COVID-19, including the ArriveCAN app," and "(w)e subsequently received a Privacy Compliance Evaluation from PHAC and have provided recommendations. We also requested more information and are awaiting a response".[674]

288. In future, COVID Alert Canada and its PT versions could co-exist with other official PT CTAs (e.g., a Quebec-specific official app). It is an open question whether such apps would be interoperable.

289. Further, in future, COVID Alert Canada and its PT versions could be accompanied by *official* wearables. For example, on July 31, 2020, Ontario Premier Ford said he is "in favor" of the made-in-Ontario wearable "TraceSCAN", developed and owned by Facedrive (TSXV:FD,OTC:FDVRF), but "that's going to be strictly up to the federal government to decide".[675] On August 4, 2020, the Laborers' International Union of North America ("LiUNA"), which represents Ontario's construction industry, urged GoC to adopt the TraceSCAN wearable to protect Canadians in workplaces where smartphones are prohibited or not viable for contact tracing (e.g., construction industry).[676] GoC, asked if it is considering adding a wearable component to COVID Alert Canada or adopting TraceSCAN, did not respond to media requests for comment.[677]

290. **Relationship to <u>unofficial</u> DCTT (present/future).** COVID Alert Canada and its PT version(s) co-exist with unofficial DCTT, both network-level (see details above) and application-level, including CTAs and wearables. For example, as of July 6, 2020, BC-based Mimik Technology's CTA, Pandimik, was reportedly ready to be deployed and large companies were evaluating it as a back-to-work tool.[678] On August 14, 2020, Mimik CEO Fay Arjomandi said the app has been enjoying quick adoption by business clients aiming to get their employees back into workplaces.[679] On July 29, 2020, Facedrive announced the TraceSCAN wearable is being piloted in Canada's construction industry, starting in early August.[680]

COVID ALERT CANADA RELATIONSHIP TO BROADER DIGITAL "OUTBREAK RESPONSE" & HEALTH TECHNOLOGY

GOC & PT GOVERNMENT ENGAGEMENT IN GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE ("GPAI")

291. On June 15, 2020, GoC, Quebec, and representatives of the 14 other founding members of the Global Partnership on Artificial Intelligence ("GPAI") announced the official launch of this initiative. GPAI will conduct various activities, including "investigate how AI can be leveraged to respond to and recover from COVID-19", and its contributing Canadian experts include Yoshua Bengio, Founder and Scientific Director of the Mila research institute on AI (developer of the COVI app).[681]

PT GOVERNMENTS' HEALTH DATA PLATFORMS (OVERALL)

292. PT governments are building and enhancing their health data platforms (overall) to better respond to the COVID-19 pandemic. An example is the Ontario government, which is working with "local public health units and other health care partners to implement effective policies to respond to the COVID-19 outbreak"[682] and has announced its *expansion of data collection* to help stop the virus' spread.

293. On May 29, 2020, the Ontario government announced a new phase of its "COVID-19 testing plan"[683], subsequently described as a "significant expansion of testing (that) will go hand-in-hand with local public health units' ongoing case and contact efforts [684].

294. On June 4, 2020, the Ontario government announced the appointment of a Special Advisor to develop the new "Ontario Health Data Platform" (formerly known as PANTHR). According to a news release, the platform will "provide recognized researchers and health system partners with access to anonymized health

data" – specifically "better and more consistent population data" that is "secure" and "used in a privacy-protected way" – to "allow them to better detect, plan, and respond to COVID-19" and "support projects from the Ontario COVID-19 Rapid Research Fund".[685] The collected data will help with "increasing detection of COVID-19", "discovering risk factors for vulnerable populations", "predicting when and where outbreaks may happen", "evaluating how preventative and treatment measures are working" , and "identifying where to allocate equipment and other resources".[686] The Ontario Health Data Platform "is being developed in consultation with the Ontario Privacy Commissioner"[687], however no information is provided on its potential relationship to *digital* contact tracing initiatives (official or unofficial).

295. On June 15, 2020, the Ontario government announced its proposal of "a regulatory change to mandate the reporting of data on race, income, language and household size for individuals who have tested positive for COVID-19" to "help ensure the province has a more complete picture of the outbreak".[688] The News Release states[689]:

> *"Under these proposed changes, individuals who have tested positive for COVID-19 infection will be asked additional questions about their race, income, languages spoken, and household size. Individuals can choose not to answer any or all of these questions. Individuals' privacy is protected as it is for all information currently collected on other diseases (...) Anonymized data will be made available to recognized researchers through the Ontario Health Data Platform, but protecting individuals' privacy protection is the priority."*

No information is provided on the potential relationship between these proposed changes, *digital* contact tracing initiatives (official or unofficial), or *digitally-assisted manual* contact tracing efforts.

PT GOVERNMENTS' "ENHANCED" MANUAL CONTACT TRACING EFFORTS

296. The COVID Alert Canada website emphasizes the app "is just one part of the public health effort to limit the spread of" the virus and "does not replace manual contact tracing" by local PHAs.[690] The Ontario government says that COVID Alert Ontario "is a key tool to strengthen Ontario's comprehensive case and contact management strategy, *Protecting Ontarians through Enhanced Case and Contact Management*"(see details below).[691]

297. In some regions (e.g., Ontario) and cities (e.g., Toronto), manual tracing has struggled to get up to speed (see details below).[692] June 18, 2020 "mark(ed) 100 days since the World Health Organization declared COVID-19 a pandemic" and the "day that Canada officially recorded more than 100,000 cases of COVID-19, as provinces continue to ramp up testing to understand accurate levels of infection".[693]

298. Questions have been raised about PT governments' manual contact tracing efforts. For example, on June 6, 2020, CBC questioned why more than 50,000 Canadians who volunteered pursuant to GoC's "National COVID-19 Volunteer Recruitment Campaign" to help with manual tracing and case data collection and reporting are not being used, especially by the "hardest-hit provinces" (Ontario and Quebec).[694] To support and strengthen their manual contact tracing efforts, PT governments are:

- deploying PHA case and contact data management systems; and
- implementing recovery plans that require, recommend, or rely on businesses (including online-only) to support contact tracing.

PT PHA CASE & CONTACT DATA MANAGEMENT SYSTEMS

299. PTs are implementing digitally-assisted manual contact tracing. For example, on June 18, 2020, Ontario announced that together with COVID Alert Ontario it is "providing additional contact tracing staff" and:

> *"implementing a new user-friendly case and contact management system that will integrate with COVID-19 laboratory results from the Ontario Laboratory Information System (OLIS) data, making*

current processes significantly more efficient and reducing the administrative burden for public health unit staff. A single central system will enable the province to identify province-wide regional trends and hotspots, while protecting personal health information. Custom-built on the Salesforce platform, the new system will also allow for a remote workforce, enabling contact tracing to be quickly ramped up when required."[695]

No details are provided on the Salesforce platform. Notably, as of June 18, Ontario's manual contact tracers were reaching approximately 97% of new COVID-19 cases within one day.[696]

300. PIAC's research indicates that Salesforce is involved in COVID-19 direct response by governments around the world. Salesforce is "an online solution for customer relationship management, or CRM".[697] The company is involved with global government efforts to respond to the COVID-19 pandemic, because "(t)here is probably no time in recent memory when up-to-date, accurate data has been more important – or more in demand from the broader public".[698]

301. According to Salesforce's official website, key "government and general public" initiatives include: "working closely with officials from a wide variety of local governments (…) to state governments (…) to national entities like the National Health Services (NHS) in the UK… to use their data more effectively and/or make it available to the public"; and "(t)he COVID-19 Data Resource Hub, first published in March, (which) continues to be a resource for government, NGOs, and the general public".[699] The "customer success stories" section of the Salesforce website recognizes "(t)he state of Rhode Island is a trailblazer in testing and contact tracing efforts" because it "move(d) its testing and contact tracing system to the cloud", specifically to "**Salesforce's Customer 360 for Government**".[700] PIAC believes there is a reasonable chance this system is the Ontario government news release-referenced "new system" that is "custom-built on the Salesforce platform".

302. Saleforce's Customer 360 for Government gives Rhode Island's Department of Health "a comprehensive record of each and every COVID-19 case across the state, and allows for a more integrated and adaptable solution to the pandemic", and works like this[701]:

"A Rhode Island resident starts experiencing COVID-19 symptoms and they call their healthcare provider. If the patient's symptoms warrant a test, the physician can log into an online portal built on Community Cloud and Lightning Scheduler, look through available days and times at nearby testing sites, and schedule accordingly. Relevant details, such as symptoms and basic demographics, are captured in a profile-like record in Health Cloud at the time of test-scheduling, allowing the team to potentially have a fuller picture of how positive and negative results are broken down within the community. The system also allows Rhode Islanders to 'self-schedule' tests.

Rhode Island is beginning to leverage built-in API capabilities of Salesforce to feed laboratory test results into the system. If the results are positive, they are added to the workflow of Rhode Island Department of Health case investigators, who then follow up with the individual to explain that they need to enter isolation and see if they would be open to participating in the state's contact tracing effort. For those who are willing, case investigators can sign up the individuals up for automated symptom monitoring which will let the individual know when they are ready to end isolation. This triggers a daily SMS text message containing a survey (sent via a third-party system), which individuals can use to report any changes in symptoms and request services such as housing and food support to help ensure they can succeed with isolation. The results are integrated within Salesforce, and built in logic helps drive the functionality. Every day the list of individuals needing quarantine or isolation support services is provided to RI's local United Way 211 to help connect the individual with the support they need; efforts are underway to integrate this process electronically (…)

In a desire to continuously improve the response, the state is starting to also measure the number of cases, how long it takes to process a case, testing of the workforce, and so on. The number of

users can be ramped up or ramped down (…) And, since the platform is built in the cloud, this can all be done via a remote work environment."[702]

303. PIAC's research also indicates that Salesforce is involved in COVID-19 direct response by businesses around the world. In particular, Salesforce supports businesses providing "private sector direct response" to COVID-19, by "help(ing) deliver data solutions tailored to two pressing needs": "(f)or organizations needing to make decisions around employee health and returning to work" a HR analysis template that combines HR and COVID-19 data; and "(f)or healthcare organizations… the healthcare starter", which "includes a COVID-19 dashboard, metric workbook, and instructional materials for key measures such as test administered results, and metrics applicable to any EHR".[703]

PT GOVERNMENT RECOVERY PLANS REQUIRING/RECOMMENDING BUSINESSES TO PROVIDE DATA

304. As of June 2020, PT governments are issuing COVID-19 recovery plans that require or recommend businesses to support contact tracing efforts by collecting personal data on their customers and advising on ways they can do so ("contact tracing advice").[704] This contact tracing advice is inconsistent across Canada, being specific and detailed in some PTs (e.g., BC) and general and broad in others (e.g., Ontario), making it unlikely to have a meaningful impact on public health, potentially privacy-invasive for Canadians as consumers, and legally risky for businesses to adopt.[705]

305. For example, as of July 16, 2020, the NB government was finalizing formal guidelines for businesses and other organizations that are mandated to collect the personal information of patrons for COVID-19 contact tracing purposes, after the NB Privacy Commissioner raised concerns about the lack of clarity and risk of a breach.[706] CCLA's Brenda McPhail noted this type of data collection is unprecedented thus "we don't have the understanding of the rules in place about how it's going to be used" which "should have been put in place first, at the beginning of this process because otherwise, this is a breach waiting to happen" (e.g., stalkers or "police fishing expeditions") and worried that, absent formal guidelines, what might seem to be mild surveillance would become embedded and expanded over time.[707]

306. Further, effective August 7, 2020, the Ontario government mandated bars and restaurants to take the personal information of patrons to "support case and contact tracing" by requiring bars and restaurants (and also tour boat operators) to keep client logs for a period of 30 days and to disclose the client logs to the medical officer of health or an inspector under the *Health Protection and Promotion Act* on request.[708] Former Ontario Privacy Commissioner Ann Cavoukian expressed privacy concerns, because lists of personal information are "rarely deleted securely", "could get into the wrong hands", and "could compromise you in some way that we can't anticipate".[709]

307. Canadian PHAs are also accessing location and personal data gathered by *online-only* businesses. For example, according to media reports, PHAs across Canada are "using data from Uber to beef up their contact-tracing efforts"[710]. In particular[711]:

- The week of July 13, 2020, Uber globally launched a service (aka "new portal"), for exclusive use by PHAs, free of charge, that provides quick access to data (sought based on trip receipts or passenger names) on drivers/riders who may have interacted with an infected person. PHAs can request information on a driver or rider they know or suspect has tested positive for COVID-19, or who they suspect has come in contact with someone with the virus, and advise Uber on how to manage a user who is thought to have come in contact with the virus (e.g., by locking their ride-sharing app for 14 days). Users with a confirmed positive diagnosis are automatically blocked from Uber for at least 14 days but otherwise Uber follows PHAs' recommendations. Uber may provide PHAs with names and contact information of other Uber users whom a COVID-19-positive driver or rider may have encountered.
- The service is an "extension of Uber's law enforcement and public safety portal" that "provides law enforcement officials with user data when Uber is legally compelled to, or when its team of …law enforcement experts determines it's in the interest of the public safety to do so". According to a

disclosure notice on Uber's website, it will disclose information if it "has a good-faith belief that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency" and "(i)t is Uber's position that outbreaks of infectious disease where public health officials have declared a public health emergency under applicable law qualify as emergencies". Uber also said it may share data voluntarily with PHAs if it is related to a public health emergency, even absent a government-declared state of emergency. Uber considers COVID-19 to be an emergency involving danger of death or serious physical injury.

Ann Cavoukian contends that Uber's involvement in contact tracing raises privacy concerns, because "it is completely unacceptable that the judgment for these kinds of calls on disclosure of sensitive personal health information is going to be made by (Uber)", especially since Uber is not getting users' explicit consent to share their data with PHAs, which she said should happen every time someone uses the ride-sharing app.[712]

PART 5: CANADA URGENTLY NEEDS "PRIVACY-FIRST" PUBLIC POLICY ON DCTT RELATED TO COVID-19 & FUTURE PANDEMICS, IMPLEMENTED VIA ACCELERATED *PRIVACY LAW REFORM* & INTERIM *PRIVACY RISK-MITIGATION STRATEGIES* ("PIAC RECOMMENDATIONS")

308. In light of the foregoing description and analysis of the state of Canadian COVID-19 DCTT in global context, **PIAC recommends that FPT governments should adopt a "privacy-first" public policy on DCTT and broader digital health technologies related to COVID-19 and future pandemics ("Privacy-First Policy on DCTT"), comprised of a set of privacy principles that is built on current Canadian privacy law and global best practice in privacy policy responses by democratic governments.** This policy approach would strike the *right* balance between (the individual right to) privacy and (the public interest in) public health-safety.

309. Further, **PIAC recommends the Privacy-First Policy on DCTT should be implemented via accelerated, broader privacy law reform that bridges the digital privacy gap and interim privacy risk mitigation strategies deployed by governments, regulators, and businesses. These recommendations (collectively, "PIAC recommendations") are detailed below.**

PUBLIC POLICY SHOULD SET CONDITIONS FOR RESPONSIBLE DCTT USE IN THE PUBLIC INTEREST, TO MITIGATE DCTT RISKS (ESP. PRIVACY) TO GREATEST EXTENT POSSIBLE

310. **PIAC recommends that Canadian public policy (FPT) must set the conditions for responsible DCTT use, in the public interest, to mitigate all DCTT risks (especially privacy) to the greatest extent possible in the specific circumstances.**

CANADA'S PUBLIC POLICY APPROACH TO COVID-19 DCTT WAS SUBOPTIMAL

311. Canada's public policy approach to COVID-19 DCTT was flawed, in that FPT governments decided on technological options for digital contact tracing before transparently deciding on policy options.

312. **Political debate on DCTT.** As noted, the *political* debate on official DCTT began in earnest in early May 2020, after its initial deployment, and focused on the technology, specifically the proper level and type of CTA.

313. **Public debate on DCTT.** As of mid-May 2020, the *public* was engaged in a "policy conversation about deploying" DCTT, specifically apps, focused on their overall "pros and cons"[713], however privacy was not a major concern. On May 13, 2020, Teresa Scassa observed that while "Canada is debating how to use technology" to respond to the COVID-19 pandemic, "little public sentiment seems to have galvanized around contact-tracing apps" and privacy, notwithstanding "the attention already paid to privacy in Europe and elsewhere" and the May 1 launch of ABTraceTogether, which "should set off both privacy and transparency alarms". The absence of a privacy alarm persisted until at least May 27, 2020 – two weeks

before GoC endorsed COVID Alert Canada – when the Canadian Centre for Cyber Security, a division of the Communication Security Establishment ("CSE") asserted: "We *expect* that privacy concerns will *likely initiate* passionate public debates (…) on the expanding use and effectiveness of surveillance technologies to combat the ongoing COVID-19 pandemic".[714]

SOUND PUBLIC POLICY APPROACH TO DCTT IS VITAL TO ENSURE ALL RISKS OF DCTT (ESP. PRIVACY) ARE MITIGATED TO GREATEST EXTENT POSSIBLE

314. Due to the inherent and globally-realized risks of DCTT, including CTAs, it is vital for Canadian governments to ensure the vulnerabilities of DCTTs deployed in Canada in response to COVID-19 and future pandemics are mitigated to the greatest extent possible.

315. **Sound policy approach to DCTT (overall).** "Canada has a reputation as a second- or third-mover in a lot of policy arenas, to the frustration of some and the admiration of others"[715] and it has taken this approach to COVID-19 DCTT, greeting it with more skepticism than many other countries[716] and with correspondingly delayed adoption and deployment of official contact tracing apps. However, mitigating the risks of DCTT to the greatest extent possible means that before it is deployed – or at least massively deployed – "we must do the policy work to set conditions for (its) use", which "is much more challenging than the technical mechanics" and entails transparently asking and answering hard questions[717]. For contact tracing apps:

> *"A defensible policy approach … will openly and publicly ask and answer questions about the proper conditions for their use, and the cessation of their use. At a high level, these include: What do we want use of the app to achieve? How will we know when it's working? How will we know when it's being abused? How will governments make sure compromises made during extraordinary circumstances don't become normalized when they're over? And how will governments use the information gleaned from a health crisis to shape access to the economy and social support programs?"*[718]

By corollary, Canadian governments should not decide on technological options for digital contact tracing before openly and publicly deciding on policy options[719] (a recommendation that, as noted, has not been heeded).

316. This sound policy approach to DCTT is justified on several grounds. First, "(t)he goal is not a good tech deployment; the goal is a healthy, free public"[720]: "One of the main reasons we need rigour in the development of policy that defines how governments make large, sweeping decisions — like when to lock down, test and trace people — is to ensure that we're framing response efforts around the public interest."[721]

317. Second, this policy approach to DCTT aligns with Canada's embrace of "Open Government" principles[722], while enhancing trust, thereby fostering wider adoption of DCTT, and increased effectiveness:

> *"Canada prides itself on being part of the open government movement. This should involve being open about its thinking and decision-making processes along the way through this pandemic, including milestones and decision points related to any use of these apps, should they be deployed. By taking the time to document a full policy approach to the potential use of these apps prior to any decision about deployment, and making it public for scrutiny, governments can lean into the ongoing development of public trust — trust they cannot afford to lose as they continue to adapt to ever-changing information about the disease and a raft of other unknowns."*[723]

318. Third, policymakers likely have one chance to get DCTT interventions right:

> *"Governments might not have a second chance to get an intervention right — failure now could breach public trust for the foreseeable future… Even in a crisis, a 'try-everything' approach is dangerous when it ignores the real costs, including serious and long-lasting harms to fundamental rights and freedoms, and the opportunity costs of not devoting resources to something else."*[724]

319. Finally, painful policy debates and difficult policy decisions made now are critical to ensuring appropriate DCTT to minimize damage from COVID-19 and future pandemics, which are a certainty. This is especially true with respect to contact tracing apps:

> *"Making the right tradeoffs between privacy, security, design, and policy for this generation of contact tracing apps will be critical to limiting damage from the current pandemic. But the decisions made now will also likely form the foundation of future contact tracing apps. If the coming COVID-19 apps are widely embraced and prove their value, many painful and time-consuming policy and technical debates could be avoided when the next pandemic hits. And (…) we can be sure there will be a next time. 'If you needed to do this again, could we do it faster next time?' (…) 'Could we have the code for the app sitting there so that it's easy to do it again quickly? Is the integration into the health system maintained so that next time we don't have to start from scratch? The expertise we are developing right now, the knowledge, is going to be important even after we are past this crisis.'"*[725]

320. **Sound <u>privacy</u> policy approach to DCTT.** In particular, a sound privacy policy approach to DCTT "seems a minimum requirement" in an environment where technology decisions must be made quickly and "individuals are asked to sacrifice some measure of privacy for the public good".[726]

321. A deliberate and transparent FPT government decision on the extent of this privacy sacrifice (a "balance" question that is revisited below) is *possible* even in a pandemic, when "the tradeoff between speed and perfection shifts radically" and we don't "have the luxury of interminable debates as developers and engineers twea(k) the system to respond to every (privacy) objection"[727]. It is also *necessary*, to ensure "political accountability re: public health and tech"[728] choices that have potentially irreversible long-term consequences for privacy (e.g., if Canadians' privacy rights are significantly violated it could be difficult if not impossible to put the toothpaste back in the tube). CIGI senior fellow Bianca Wylie emphasizes that political accountability is particularly important for *official* CTAs (aka "government apps"), which are inherently political, and that it requires Canadians to know "how the data flow works, and where it's different from other data collection and use processes".[729]

322. It cannot be sufficiently emphasized that privacy decisions on DCTT properly belong to democratic governments and not Big Tech. In the case of COVID Alert Canada and other global official apps built on the Google/Apple API, the design decision on privacy, which constrains governments' ability to collect useful data, was first and foremost made by Big Tech, which **"**raises serious questions about democratic oversight of critical global infrastructure"[730]:

> ***"****Key decisions about what aspects of privacy to protect should not be made by shareholder-driven multinational companies unconstrained by traditional accountability mechanisms, instead of democratically elected governments. While the COVID Alert app is a valuable tool in the ongoing fight against a global pandemic, we should be mindful of the larger implications it — and tools like it — have for the structure of our society, how we can and should run it, and who controls the reins."*

323. The need for political accountability on the public health and tech response to COVID-19 is demonstrated by a July 2020 Globe and Mail investigation entitled "'Without early warning you can't have early response': how Canada's world-class pandemic alert system failed"[731]. It found that Canada's pandemic alert system, Global Public Health Intelligence Network ("GPHIN"), lauded by WHO as "the foundation" of the global pandemic early warning system, failed to warn about the COVID-19 pandemic because GoC "effectively switched (it) off" in May 2019 by shifting priorities inside Public Health, leaving Canada "conspicuously unaware and ultimately ill-prepared":

> *"It's not easy to know the consequences of such decisions (…) Mr. Garner, the former senior science adviser at Public Health, says he believes Canada's early response to the outbreak – which has been criticized for being slow and disorganized – was a product of the many changes he saw made to the department (…) which slowed down its ability to react effectively – and with*

maximum urgency. 'All of these things have tragically come home to roost,' Mr. Garner said. 'Not be overdramatic, but Canadians have died because of this.'"[732]

As of July 30, 2020, Canada's auditor general will reportedly investigate GoC's mishandling of GPHIN.[733] (On a separate but related note, as further proof of Big Tech's incursion into the global health market, in 2008, Google offered to buy GPHIN from GoC due to its impressive data-mining capabilities.[734])

324. **Role of public interest groups and policy experts.** Public interest groups and policy experts have a crucial role to play in sound DCTT policy discourse. "It's critically important for the policy community to do what it does best in this challenging context: bring a broad range of expertise and perspectives to defining, prioritizing and achieving public-interest health outcomes."[735] The reasons, as noted, are: transparency; democracy; rule of law; privacy law; and avoiding exploitation of vulnerable persons.

PRIVACY-RESPECTING DCTT IS IMPORTANT TOOL TO FIGHT COVID-19 & FUTURE PANDEMICS

325. PIAC believes that *privacy-respecting* DCTT is an important tool to fight COVID-19 and future pandemics. Digital contact tracing, done correctly and with eyes wide open, is "one more tool to detect and fight an invisible adversary"[736], COVID-19, the latest but likely not the last pandemic to threaten "the health, economy, and social cohesion of societies on a global level, generating a crisis response"[737].

326. Privacy-respecting DCTT is important for its own sake, and because it has short- and long-term societal benefits, including the following.

327. **Bolsters trust, thus boosting adoption and effectiveness**. The more privacy invasive DCTTs are, the more personal data they collect, and the easier they make contact tracing, case investigation/management, and epidemiological learning about COVID-19. The trade-off is that privacy-respecting DCTT bolsters the trust of populations, thus boosting DCTT adoption and effectiveness. According to a Japanese government official from the IT taskforce, Norihiro Kiyoshige, Japan's official Bluetooth decentralized (Google/Apple API) contact tracing app "Cocoa", was chosen for this reason: "It's true that the more invasive an app is, the easier it makes contact-tracing. But then, such an app will most likely be snubbed by many prospective users" therefore "(w)e thought guaranteeing privacy and assuring people of its safety would be the most effective way to boost the app's penetration".[738]

328. **Prevents exceptions to civil liberties in a crisis from persisting past it.** Privacy-respecting DCTT prevents exceptions to civil liberties in a pandemic crisis from persisting past it. History has shown that new surveillance technologies and exceptions to civil liberties protections made during a time of crisis often persist beyond the crisis itself[739] and "further normalize the surveillance of individuals by governments and private entities alike"[740]. This concern was expressed by certain Canadian privacy commissioners prior to the launch of COVID Alert Canada. On July 30, 2020, The Logic reported on its interviews with FPT privacy commissioners about the challenges of their job during the pandemic[741], in which some PT privacy commissioners worried that without proper oversight, government and business will use COVID-19 to increase surveillance:

- Newfoundland and Labrador's privacy commissioner, Michael Harvey: said "(t)he pandemic can be a justification for a detailed level of surveillance of our society to try to keep us healthy", "(t)he amount of data that corporations and our public bodies are collecting on us is increasing pretty dramatically", and "(m)y concern is that (…) we end up in 2023 with governments that have used the pandemic as a foot in the door to a society that is surveilled in a much heavier way than we imagined".
- New Brunswick ombudsman Charles Murray: said "(w)e all expect that the world after the pandemic will not be the same as it was before" and "(w)e should use this opportunity to show how we can achieve what we need to achieve without increasing surveillance".

329. Privacy safeguards for DCTT can help to ensure that DCTT and related privacy sacrifices made by Canadians during COVID-19 and future pandemics have a crisis-limited lifespan and that "the word 'crisis' does not

become a magic talisman that can be invoked to build new and ever more clever means of limiting people's freedoms through surveillance".[742] The **key message is "privacy should not be a casualty":**

> *"As a result of the COVID-19 pandemic, most people accept and appreciate the need for extraordinary steps to protect the most vulnerable and the community at large. The measures being developed in response to the virus must, however, take privacy issues into account, have one eye on the long-term use of the data being collected, and ensure privacy is not another casualty of the crisis."*[743]

DCTT REIGNITES POLICY DEBATE OVER HOW TO BALANCE PRIVACY & PUBLIC HEALTH-SAFETY: HOW MUCH PRIVACY SHOULD INDIVIDUAL CANADIANS SACRIFICE FOR PUBLIC GOOD IN A PANDEMIC?

330. The need for privacy-respecting DCTT reignites the public policy debate over how to *balance* (the individual right to) privacy and (the public interest in) public health-safety or, in other words, how to achieve the right balance between personal information protection for privacy purposes with personal information collection for public health-safety purposes. Put differently still, **the core public policy question is: how much privacy should individual Canadians sacrifice for the public good in a pandemic?**

331. This debate is often framed simplistically as "striking a balance between privacy and health". It is also framed problematically as "privacy *versus* public health", which erroneously suggests that DCTT is a binary choice between privacy or public health and thus cannot or should not aim to achieve both. From this binary perspective, "privacy-respecting DCTT" is an oxymoron.

332. This erroneous framing of the debate is reflected in the pejorative labelling of public interest advocates who call for DCTT privacy risks to be mitigated as "privacy fundamentalists" arguing for DCTT that is void of *any* privacy concerns, thereby making any type of tracing impossible.[744] PIAC does not believe that privacy (or security) risks of DCTTs *could be* eliminated, because these risks are "intrinsically a part of any networked technology"[745], or *should be* eliminated, because this would likely eliminate all of their public health benefits. As Dr. Ian Levy, Technical Director of the UK National Cyber Security Centre says with respect to contact tracing apps, "an app that provides fantastic provable privacy but doesn't help stop the spread of the disease isn't a useful tool".[746]

333. Rather, PIAC believes that in a democratic polity like Canada, it is necessary and possible for public policy on DCTT to strike a balance between public health and privacy: governments (notably, PHAs) must effectively and efficiently address threats to public health and safety, which requires personal information about citizens; and citizens must be able to trust that their personal information will be collected, used, and disclosed by the government – and its private sector "partners" – pursuant to rules that preserve their (human right to) privacy *to the maximum degree possible in the circumstances*.

334. Further, PIAC believes that Canadian governments can perform this balancing exercise by transparently identifying and rigorously evaluating all the costs/benefits of DCTT for PHAs and Canadians with the aim of determining "acceptable" privacy risks, using a set of privacy principles. This approach, which could be adapted for particular types of DCTT and specific pandemics, according to their epidemiology, would ensure responsible DCTT use that is in the public interest:

> *"Canadian governments have an opportunity to lead by example (…) in deploying the highest standards of privacy (…) In an age where technology platforms can help amplify mistrust and division, successfully building a regime with these robust protections may help prove out a larger point: that well-designed and -governed technology, developed and used transparently and responsibly in the public interest, can build trust and protect our democracy."*[747]

335. Finally, PIAC believes this balancing exercise would be far easier to implement if the "privacy by design (PbD)" principle – which in a nutshell "requires designing a system or process in a manner that protects the

privacy rights of individuals, rather than considering the associated privacy implications of a system or process only after deployment"[748] – was an explicit legal obligation under Canadian privacy law, as it is under the GDPR (Article 25).[749] However, we note that unless and until PbD is made an explicit legal obligation, according to privacy law experts: "Canadian *organizations* should understand PbD as a legal obligation under the GDPR and as a Canadian privacy principle, as well as PbD's implications for operations and impact on relationships with suppliers, customers and the public at large."[750]

STRIKE THE *RIGHT* BALANCE WITH "PRIVACY-FIRST" PUBLIC POLICY ON DCTT THAT STRENGTHENS PRIVACY PROTECTIONS, BUILDING ON CURRENT CANADIAN PRIVACY PRINCIPLES & GLOBAL BEST PRACTICE IN PRIVACY POLICY RESPONSES TO COVID-19

336. **PIAC recommends that FPT governments should strike the *right* balance between public health-safety and privacy by adopting a "privacy-first" policy on DCTT and related data-driven technologies ("Privacy-First Policy on DCTT") that:**

- **prioritizes and protects privacy[751]; and**
- **comprises a set of privacy principles that strengthens privacy protections by building on:**
  - **current *Canadian privacy principles* (see details below); and**
  - **global best practice in *privacy policy responses* by democratic governments, and *recommendations on privacy policy responses* by global experts, to COVID-19 DCTT ("global privacy policy responses to COVID-19 DCTT").**

GLOBAL PRIVACY POLICY RESPONSES TO COVID-19 DCTT: CAREFULLY CONSTRAINED NETWORK-LEVEL INITIATIVES & VOLUNTARY BLUETOOTH DECENTRALISED APPS PRIORITIZING EFFECTIVENESS, NECESSITY & PROPORTIONALITY

337. **Global privacy policy responses to COVID-19 DCTT by governments and recommendations by experts, at the supranational and national level, are evolving rapidly. However, to date, these favour carefully constrained network-level initiatives and voluntary, decentralized Bluetooth apps that prioritize effectiveness, necessity, and proportionality.** Notably, these responses are rooted in two vastly different legal approaches to privacy: "only restrict the free flow of information if there's solid justification to do so"[752] (US approach); and "the world's toughest rules to protect people's online data"[753] pursuant to GDPR (EU approach).

SUPRANATIONAL GOVERNMENT PRIVACY POLICY RESPONSES

338. There have been some supranational government privacy policy responses to COVID-19 DCTT, particularly at the European Union ("EU") level, including the following.

WORLD HEALTH ORGANIZATION ("WHO")

339. WHO has issued "Interim Guidance" on contact tracing in the context of COVID-19, including a May 2020 guidance on "contact tracing in the context of COVID-19"[754] ("Contact Tracing Guidance") and June 2020 guidance on "digital tools for COVID-19 contact tracing"[755] ("Digital Contact Tracing Guidance").

340. The Contact Tracing Guidance stresses that "data protection, and data privacy must be considered at all levels of contact tracing activities (…) and when implementing contact tracing tools". In particular, "(s)afeguards must be in place to guarantee privacy and data protection in accordance with the legal frameworks of the countries where systems are implemented" and "digital tools used for contact tracing should be assessed before use to ensure safeguarding data protection according to national regulations".

341. The Digital Contact Tracing Guidance recognizes that "the implementation of digital technologies in contact tracing carries the potential to do harm through privacy breaches" and "(i)t is therefore important to have sufficient regulatory oversight" of DCTT. Regarding DCTT overall, "WHO recommends that users of digital tools should participate on a voluntary basis and that written consent is always obtained. Privacy concerns about the disclosure of personal data need to always be addressed. Data processing agreements must disclose which data are transmitted to third parties and for what purpose." Regarding contact tracing apps, WHO emphasizes "(t)here are many privacy issues regarding the disclosure of location history, case and contact status, and possibly other personal data", "(p)rivacy concerns and data protection need to be carefully considered with location-based approaches" , and "(u)sing symptom tracking tools for contact tracing requires careful consideration of data ownership and of privacy and data protection".

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT ("OECD")

342. In April and May 2020, OECD published recommendations on privacy policy responses to COVID-19, including "Tracking and tracing COVID: protecting privacy and data while using apps and biometrics"[756], which recommends that CTAs "should be implemented with full transparency, in consultation with major stakeholders, robust privacy-by-design protections, and through open source projects (where appropriate)" and governments should consider:

- the legal basis for using CTAs, which "varies according to the type of data collected (e.g. personal, sensitive, pseudonymised, anonymised, aggregated, structured or unstructured)";
- whether use of CTAs and subsequent data collecting is proportionate, how the data is stored, processed, shared and with whom (including security protocols), the quality of collected data, and whether it is "fit for purpose"; and the data retention period, which should be "only for so long as is necessary to serve the specific purpose for which it was collected"; and
- whether adopted approaches are "implemented with full transparency and accountability".

EUROPEAN UNION ("EU")

343. EU institutions have issued privacy policy responses to COVID-19 DCTTs that favour a cross-EU approach comprised of voluntary, decentralized Bluetooth apps and network-level contact tracing using anonymous, aggregated location data to model and predict virus spread, with involvement of national PHAs, and subject to a specific timeframe.

344. **April 2020.** In April 2020, the European Parliament and European Commission ("EC") presented a joint COVID-19 exit plan[757]. The European Parliament endorsed the decentralized approach to *contact tracing apps*, stating "generated data are not to be stored in centralised databases, which are prone to potential risk of abuse and loss of trust and may endanger uptake throughout the Union" and demanding "that all storage of data be decentralised".[758] The EC issued a guidance on data protection and privacy implications for contact tracing apps[759] that urges Member States to ensure their apps are "voluntary, transparent, temporary, cybersecure, using pseudonymised data (…) rely on Bluetooth technology and (are) interoperable across borders as well as across operating systems"[760] and comply with EU data protection and privacy rules. The EC issued an accompanying "EU toolbox" reflecting the latest best practices in the use of apps[761]. Member States are expected to report on their actions by May 31, 2020 and EC will publish periodic reports starting in June 2020, recommending action or phasing out of measures that are no longer necessary.[762] Additionally, the EC announced it is "developing a common approach for modelling and predicting the evolution of the virus through *anonymous and aggregated mobile location data*", to be transmitted by mobile phone operators to the Joint Research Centre ("JRC") for processing and modelling, which will not be shared with third parties and only be stored for the duration of the pandemic.[763] Further still, the EDPB issued guidelines on the use of "location data and contact tracing tools"[764] ("EDPB Guidelines 04/2020") and on the processing of health data for purposes of COVID-19 scientific research[765].

345. The EDPB Guidelines 04/2020 warn that while location data and contact tracing tools "can be key components in the fight against COVID-19 (…) one should be wary of the 'ratchet effect'" and "one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights; we can achieve both"[766], in key ways including:

DCTT (Overall)

- Use measures "to empower, rather than to control, stigmatise, or repress individuals", guided by "general principles of effectiveness, necessity, and proportionality".[767]
- Ensure measures "are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation".[768]

Location Data (Network- And Application-Level)

- Give "preference (…) to the processing of anonymised data rather than personal data" (which "is often mistaken for pseudonymization"), meaning "the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any 'reasonable' effort".
- Acknowledge that "location data (…) are known to be notoriously difficult to anonymise" and aim for "robust" anonymisation, which requires removing the ability for "singling-out (isolating an individual in a larger group based on the data)", "linkability (linking together two records concerning the same individual)", and "inference (deducing, with significant probability, unknown information about an individual".[769]

Contact Tracing Apps

- Before implementing, conduct and publish a data protection impact assessment ("DPIA").[770]
- Should be voluntary, proximity-based[771], and decentralized.[772]
- Algorithms "should work under the strict supervision of qualified personnel", "be auditable", and "be regularly reviewed by independent experts".[773]
- Source code "should be made publicly available for the widest possible scrutiny."[774]

346. As noted, GDPR Article 25 makes PbD an explicit legal obligation for DCTT. Article 25 is limited by its application to controllers of personal information ("data controllers") and, to some degree, processors ("data processors"), but not to manufacturers of the technology ("suppliers").[775] These legal distinctions, applied to DCTT, beg the fundamental question: who is the "data controller", "data processor" and "supplier" in any specific situation? This question is especially pertinent in the case of *official* apps that are *built or deployed* as *public-private partnerships*. In this regard, EDPB Guidelines 04/2020 recommends "(t)o ensure accountability, the controller of any contact tracing application should be clearly defined" (noting potential controllers include but aren't limited to PHAs) and "if the deployment of contact tracing apps involves different actors their roles and responsibilities must be clearly established from the outset and be explained to the users".[776] In contrast, the EC recommends that apps should be designed in a way that PHAs are the only controllers.[777]

347. **May 2020.** In May 2020, EU justice commissioner Didier Reynders warned that contact tracing apps must only be used for the duration of the pandemic[778]. Further, the EC released its "framework" for safe and efficient apps across the EU[779]. According to a press release, the framework:

> *"sets out that tracing apps must be voluntary, transparent, temporary, cybersecure, using temporary and pseudonymised data; they should rely on Bluetooth technology and (be) approved by national health authorities, and be inter-operable across borders as well as across operating systems. Interoperability is crucial, so that wide, voluntary take-up of national tracing apps can support the relaxing of confinement measures and the lifting of restrictions of freedom of movement throughout the EU.*
>
> *EU Citizens should be able to rely on a single app independently of the region or Member State they are in at a certain moment. Most Member States have launched or intend to launch an*

approved mobile contact tracing app designed to fulfil operational objectives that are specific to their national COVID-19 crisis management strategy. The guidelines set out these minimum requirements for approved apps to communicate with each other so that individual users can receive an alert, wherever they are in the EU, if they may have been in proximity for a certain time to another user who has been tested positive for the virus. Ultimately, this will support the gradual lifting of border controls within the EU and the restoration of freedom of movement."[780]

348. Notwithstanding the foregoing, according to European law experts: "While both the European Commission (EC) and the European Data Protection Board (EDPB) consider the decentralized approach to be 'more in line with the [data] minimization principle', they have not per se rejected the idea of a centralized solution."[781] Indeed, EDPB expressly states that "implementations for contact tracing can follow a centralized or a decentralized approach" and "(b)oth should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages" regarding their "effects on data protection/privacy and the possible impacts on individuals (sic) rights".[782] Moreover – as demonstrated above in Part 3 – the idea of a single, pan-EU app "seems more unlikely everyday (sic), or even that of compatible and interoperable centralized and decentralized apps across EU Member States"[783].

349. **June 2020.** On June 16, 2020, at its 32nd Plenary Session, EDPB adopted a "Statement on the Data Protection Impact of the Interoperability of Contact Tracing Apps"[784] ("EDPB Statement on App Interoperability"), building on the EDPB Guidelines 04/2020, and a separate "Statement on the Processing of Personal Data in the Context of Reopening the Schengen Borders"[785] ("EDPB Statement on Processing Personal Data). Key elements of these statements, according to EDPB's news release[786], include:

<u>EDPB Statement on App Interoperability</u>

- More in-depth analysis of key issues such as "transparency, legal basis, controllership, data subject rights, data retention and minimisation, information security and data accuracy in the context of creating an interoperable network of applications".
- Sharing of data about infected individuals using interoperable apps should only be triggered by a user's voluntary action, interoperability should not be used "as an argument to extend the collection of personal data beyond what is necessary", and apps "need to be part of a comprehensive public health strategy to fight the pandemic, such as testing and subsequent manual contact tracing for the purpose of improving effectiveness of the performed measures".
- Ensuring interoperability "leads to a potential increased data protection risk", thus "controllers need to ensure measures are effective and proportionate and must assess whether a less intrusive alternative can achieve the same purpose".

<u>EDPB Statement on Processing Personal Data</u>

- Measures allowing a safe reopening of the borders currently envisaged or implemented by Member States include use of a voluntary contact tracing app and processing of personal data. Member States that "intend to process personal data in this context" should ensure "prior consultation with competent national supervisory authorities".
- GDPR remains applicable, processing of personal data must be necessary and proportionate, and the level of protection should be consistent throughout the European Economic Area ("EEA") (e.g., Member States should "take a common European approach when deciding which processing of personal data is necessary in this context"). GDPR principles that Member States "need to pay special attention to when processing personal data in the context of reopening the border" include: "lawfulness, fairness and transparency, purpose limitation, data minimisation, storage limitation, security of data and data protection by design and by default".
- The decision to allow entrance into a country should not only be based on "automated individual decision making technologies" and, in any case, such decisions should be "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human

intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision". Automated individual decision measures should not apply to children.

NATIONAL GOVERNMENT PRIVACY POLICY RESPONSES

350. Individual countries have adopted or are considering privacy policy responses to COVID-19 DCTT. Key examples follow.

UNITED STATES

351. In the US, there is no "baseline federal privacy legislation" and data privacy and security laws are "voluminous, differing and difficult to interpret and harmonize"[787]. The CDC has published some general guidance on DCTT, which appear to be geared towards its use by PHAs, suggesting DCTT should, amongst other things: "ensure data is secure and confidential, be able to receive input from public health authorities, facilitate identification of known contacts, and be able to send notifications of exposure in multiple electronic formats".[788] Further, multiple bills have been introduced or adopted to address the privacy implications of COVID-19 digital contact tracing. Illustrative examples follow.

352. On June 1, 2020, Republican and Democratic party lawmakers proposed the federal *Exposure Notification Privacy Act* to establish privacy requirements for *exposure notification* contact tracing apps.[789] Among other things, the bill, which is "the first visible attempt at national leadership around digital contact tracing"[790], requires: apps must be voluntary, with "affirmative express consent"; apps must minimize, de-identify, and aggregate data; apps must use data for public health purposes only, and if data is shared, require the sharing entity to adhere to the same condition; and app providers must "collaborate" with PHAs. The bill has been criticized for largely recommending measures already built-in to the Google/Apple API.[791]

353. Previously, in April 2020, Senate Republicans proposed the federal *COVID-19 Consumer Data Protection Act* about DCTT. The bill includes[792]:

- Entities: any entity or person who "collects, processes, or transfers covered data" and is also subject to the *Federal Trade Commission Act ("FTC Act")*, is a common carrier subject to the *Communications Act of 1934*, or is a non-profit organization.
- Data: prohibits "precise geolocation data, proximity data, and personal health information" unless it is aggregated, de-identified, or publicly available.
- Protection of data: requires *prior* notice and *express* consent ("notice and consent") unless there is a need to comply with legal obligations.
- Transparency: entities must publish a transparent privacy policy and issue a "public report" every 30 days.
- Right to opt-out: entities must provide a "right to opt-out" (i.e., revoke consent) and upon receiving an opt-out request, must either stop collecting/processing/transferring the data or de-identify it.
- Data deletion, de-identification, and minimization: entities must minimize data collection/processing/transfer ("use") to what is "reasonably necessary, proportionate, and limited" to the initial purpose, and must delete or de-identify data when it is no longer being used for its initial purpose.
- Security of data: entities must establish security protections for data.
- Enforcement: carried out under FTC Act regarding unfair or deceptive acts or practices.
- Pre-emption of state law: prohibits states from adopting or enforcing any law related to data (as defined above).

354. One of the bills drafted by US legislators to regulate contact tracing apps makes it illegal for any entity to discriminate against, or make unavailable goods, services, and accommodations to, individuals that choose *not* to use an app.[793] At the state level, a South Carolina-adopted COVID-19 pandemic spending bill forbids PHAs from using CTAs.[794]

FRANCE

355. In May 2020, France's *centralised* StopCovid app received preliminary support from the National Digital Council advisory board (which said it could only render a final opinion after evaluating the actual app). The app also received support from French data protection authority Commission Nationale Informatique et Libertés ("CNIL"), in its May 26, 2020 opinion on the conditions for implementing StopCovid[795] ("CNIL Opinion"), which:

- confirms the app will use pseudonymised data, not use geolocation data, and not create a database of infected individuals[796];
- finds the app reflects CNIL's April 2020 recommendations (e.g., responsibility for processing entrusted to ministry in charge of health policy and absence of negative legal consequences for non-use of app) and provides sufficient privacy measures to meet GDPR guidelines and thus can be lawfully implemented[797]; and
- recommends certain changes to ensure compliance with GDPR, including: app's utility must be re-evaluated after its launch; users must be informed how they can erase their personal data (with children and guardians informed specifically); rights to object and to be forgotten should be explicitly clarified; and free access to all source code of the app and server[798].

UNITED KINGDOM

356. As of May 27, 2020, the UK had not submitted a DPIA for its original official *centralised* contact tracing app to EDPB.[799] However, as noted, on June 18, 2020, the UK government announced it was abandoning the original app and replacing it with an app based on the Google/Apple API. The UK Information Commissioner issued a written opinion on the Google/Apple API, which[800]:

- states the API is "aligned with principles of data protection by design and by default";
- notes such apps only generate a limited amount of data and tokens are not associated with any other data that could be used to identify or locate the device user; and
- sets out similar principles to those outlined by Canadian Privacy Commissioners (see details below) and by the EDPB, including data minimization, transparency, and user control.

357. In a related UK development, on June 23, 2020, the government instructed certain businesses (e.g., bars, restaurants, and hairdressers) to record customers' personal information (e.g., contact details) and keep them for 21 days to help the NHS with contact tracing in context of its test-and-trace system.[801] The government did not provide businesses with any advice, but committed "to design this system in line with data protection legislation, and set out details shortly".[802] The Information Commissioner's Office ("ICO") said it was "assessing the potential data protection implications of this proposed scheme and is monitoring developments" and stressed that businesses, as data controllers, are not exempt from GDPR rules even under pandemic circumstances.[803]

AUSTRALIA

358. In May 2020, Australia enacted a *Privacy Amendment Act*[804] governing personal data collected by its official COVID-19 contact tracing app ("app data"), which: makes it a criminal offence to collect, use, or disclose app data except in clearly and narrowly limited circumstances; prohibits law enforcement use or retention

of app data even when agents have lawful access (pursuant to statute, warrant, or incident to arrest) to an individual's mobile device; makes it illegal to require individuals to download the official app in order to enter premises, or to receive or provide any goods or services; and bans any person outside of PHAs from collecting, using, or disclosing data from the app.[805] The Office of the Australian Information Commissioner, in its COVID-19 guidance, stated that although "the Privacy Act will not stop critical information sharing(…) [i]n order to manage the pandemic while respecting privacy, agencies and private sector employers should aim to limit the collection, use and disclosure of personal information to what is necessary to prevent and manage COVID-19, and take reasonable steps to keep personal information secure."[806]

SWITZERLAND

359. According to Switzerland-adopted legislation providing a statutory basis for the country's official CTA, "use of the app must remain voluntary and individuals who choose to not use the app cannot be disadvantaged by any authorities, enterprises or other individuals".[807]

OVERALL

360. France and other countries (e.g., Italy and UK) have established expert groups to advise on privacy and other ethical implications of contact tracing apps (e.g., UK NHS COVID-19 App Data Ethics Advisory Board).[808]

EXPERTS' RECOMMENDATIONS ON PRIVACY POLICY RESPONSES

361. Experts, both global and Canadian, have made recommendations on privacy policy responses to COVID-19 DCTT.

GLOBAL EXPERTS

362. **Policy trade-off: efficacy v. privacy.** Global privacy experts, journalists, and organizations based in democratic countries recognize there is a trade-off between privacy and the efficacy of contact tracing apps. While they are divided on which one should prevail, the majority favour privacy. For example:

- Efficacy should prevail: Forbes contributor on surveillance/security Zak Doffman writes that the "Google/Apple take-over of the whole smartphone contact-tracing ecosystem" has been "a disaster" because it "put privacy ahead of efficacy" (e.g., it can't measure distance well enough, so "the data is poor", and "there is no repository to mine", which "limits the value to those tracking the spread of infections, the localized hotspots that need a swift response to contain"), "the price for which will unfortunately be very high". He argues the proper solution is mandatory, location-based apps whose location data is "cross-referenced with CCTV and other surveillance" and with "demands for quarantining or isolation" that are "linked to rights to work and travel".[809]
- Privacy should prevail: The majority share the fundamental position of Amnesty International that "(p)rivacy must not be another casualty as governments rush to roll out apps"[810] and, more broadly, "we shouldn't allow pandemics to become pretexts" for privacy invasion[811].

363. **Guidelines and position statements**. Privacy experts and organizations have developed guidelines to assess whether contact tracing apps are "ethically justifiable". Nature's "Ethical guidelines for COVID-19 tracing apps"[812] are illustrative. To be ethical, an app must abide by four principles: be necessary, proportional, scientifically valid, and time-bound. To meet these principles, an app should satisfactorily answer key questions including:

- Is app voluntary?

- Is app temporary (defined end date), with a decommissioning process (to shut it down)?
- Is app used only for prevention (to limit spread of COVID-19) or also as a "passport" (to enable people to claim benefits or return to work) or for compliance (to enforce behaviour, with non-compliance resulting in punishment)?
- Is app open source (code publicly available for inspection, sharing and collaborative improvement) or proprietary?
- Is app equally available (free and distributed to anyone) and equally accessible (user-friendly and works on widest possible range of phones)?
- Does app require consent (choice over what and when data are shared, that can be changed at any time)?
- Is purpose of personal data collection defined and limited (to trace COVID-19 only)?
- Is personal data kept private (anonymous, de-identified, and not re-identifiable)?
- Can users erase personal data (erase data at will and all data automatically deleted at defined end date)?

364. Worldwide, "an increasing number of experts are resorting to the notion of 'decentralization' (sic) as an essential component of 'privacy preserving' software".[813] A key example is the April 2020 "Joint Statement on Contact Tracing" by global (including Canadian) scientists and researchers[814], which "strongly prefers" *proximity-based* apps over location-based apps "when available" and Bluetooth apps that are *decentralised* versus centralised, and recommends the following principles "should be at least adopted" regarding apps and the systems that support them:

- apps "must only be used to support public health measures for the containment of COVID-19" and "must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose";
- apps must be "fully transparent", meaning "protocols and implementations (…) must be available for public analysis" and "processed data and if, how, where, and for how long they are stored must be documented unambiguously" and "be minimal for the given purpose";
- app functionality must choose "the most privacy-preserving option" except when "necessary to achieve the purpose of the app more effectively", and such deviations "must be clearly justified with sunset provisions"; and
- apps *and supporting systems* must be voluntary, used with explicit consent, and "designed to be able to be switched off, and all data deleted, when the current crisis is over".

365. Global guidelines have also been created for "safe and secure" *exposure notification* contact tracing apps, such as the "Digital Contact Tracing Bill of Rights" (aka "Data Rights for Exposure Notification"[815]) written by privacy advocates, cryptologists, legal scholars, and epidemiologists in partnership with the US Digital Response ("USDR")[816] and signed by the TCN Coalition and many of its member organizations. [817] The bill of rights has two parts, general data use and individual data rights:

<u>General Data Use</u>[818]

- Apps should be "open source and/or available for audit from an independent third party", "interoperable", "fully accessible", "not discriminate" (including by "impacts of unintended consequences") and comply with "local data protection laws and regulations".
- Individuals should not have to "divulge any personal information to anyone".
- Processed data may only reveal these types of information to these types of entities: verify to "authorities" that individual is infected or healthy, with explicit consent at each verification; inform plausibly exposed individuals of potential exposure; and inform "health officials" of high level exposure trends (not individual level).

Individual Data Rights[819]

- Consent: all data provided by users should be "completely opt-in, with clear informed consent both as to the nature of what they're disclosing, how it is used, the likely impacts of disclosure and use, and any choices". Any new use requires fresh consent, and individuals can withdraw their consent at any time.
- Data ownership: users own data collected and stored on their mobile devices.
- Data collection: should be limited to achieve a defined purpose, specifically a public health purpose, and collect the minimum data necessary. *Health* data should be provided "altruistically" only, be "essential, based on epidemiological standards, for alerting others to potential exposure", and "remain completely anonymous".
- Data disclosure: data such as "location history, symptom reports, demographic information, or similar *shared with public health officials or researchers* must never be linked back to or used to re-identify individuals, *even by entities legally allowed to perform such linkage*" (emphasis added).
- Data use: data "may be aggregated so that it may not allow for the identification of individuals". Aggregate data should be "processed with privacy-protecting techniques such as differential privacy" with "methodologies and techniques (…) available for public review" and "precautions (…) taken to ensure (… it) may not be re-identified downstream", and "may be maintained for public research purposes". Data collected by, or derived from, apps "should not be monetized, shared, or used for any other non-public-health purpose", including "third party analytics, ad tracking, and other common third party data collectors".
- Data retention: should be "very clear and reasonable (…) based on epidemiological standards", "must not retain any data for longer than required to achieve the app's objective", and "have a clearly defined plan for the destruction of data once (…) apps are no longer necessary".
- Data security: data should be secured on the user's device according to industry best practices.

366. **Proposed legislation.** A group of UK academics proposed a bill that would ensure no UK resident is punished for not having a mobile device, including leaving their home without it or failing to charge it.[820]

CANADIAN EXPERTS

367. Canadian experts have made independent privacy policy recommendations, including the following.

368. **Guidelines.** The University of Waterloo Cybersecurity and Privacy Institute[821] has proposed living guidelines for contact tracing apps (e.g., simple design, minimal functionality, data minimization, trusted data governance, cybersecurity, minimum data retention, protection of derived data and meta-data, proper disclosure and consent, and provision to sunset).[822] The CPE has recommended voluntary, decentralized Bluetooth apps that follow PbD principles, are transparent (e.g., open source, independent reviews and ongoing oversight) and only collect, store, and use data that is necessary (e.g., limit data use to public health, delete data after 30 days, and delete app once pandemic is contained).[823]

369. When PM Trudeau endorsed COVID Alert Canada, a coalition of civil liberties groups and open Internet advocates – comprised of the BC Freedom of Information and Privacy Association ("FIPA"), CCLA, the BC Civil Liberties Association ("BCLA"), the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic ("CIPPIC"), OpenMedia, and the International Civil Liberties Monitoring Group – said its design appeared to meet a number of privacy principles (e.g., opt-in, anonymized, peer to peer, minimal extension of government surveillance powers, and clear limits on data use and retention). However, following reports that OPCC had not signed off on the app, the coalition said CTAs should not be deployed before FPT privacy commissioners have assessed them.[824]

370. **Legislation.** CPE has called for legislation prohibiting public and private entities from making contact tracing apps mandatory to access goods, services, employment, or housing.[825]

IMPLEMENT PRIVACY-FIRST POLICY ON DCTT VIA ACCELERATED CANADIAN PRIVACY LAW REFORM

371. **PIAC recommends the Privacy-First Policy on DCTT should be *implemented*, ideally via accelerated, broader reform of Canadian privacy law (FPT), specifically legislation. To understand this recommendation, it is necessary to start with our broader position on Canadian privacy law[826]:**

- **Canadian privacy law is complex and further complicated by COVID-19; and**
- **COVID-19 highlights gaps in Canadian privacy protections pertaining to digital technologies ("digital privacy gap"), accelerating the need for privacy law reform.**

CANADIAN PRIVACY LAW IS COMPLEX & FURTHER COMPLICATED BY COVID-19

372. Canadian privacy law is complex and further complicated by COVID-19. In a nutshell:

> *"The COVID-19 outbreak is raising questions about privacy issues during a pandemic. During a public health crisis, privacy laws still apply, but they are not a barrier to appropriate information sharing…*
>
> *In Canada, the management of public health crises is a matter involving close coordination between all levels of government. There is therefore a variety of public and private sector privacy legislation at the federal, provincial and territorial levels that govern the collection, use and disclosure of personal information. There are (federal,) provincial and territorial privacy authorities that oversee compliance with the privacy legislation in their respective jurisdictions, and some have published their own statements relevant to the matter of COVID-19…*
>
> *While privacy laws include several provisions that authorize the collection, use and disclosure of personal information in the context of a public health crisis, if you rely on them, you should be able to communicate to the persons involved the specific legislative authority under which this is done.*
>
> *Public health situations are sometimes referred to as emergencies. Under both federal and provincial laws, governments are authorized to declare formal public emergencies. Where that is done, the powers to collect, use and disclose personal information may be further extended and can be very broad. To understand the impact of such legislation on privacy, one has to read its specific terms. Normal privacy laws apply unless emergency legislation provides otherwise."*[827]

373. A high-level, non-exhaustive overview of Canadian privacy law is provided next. This overview does not reflect developments following the date of this document's publication, and PIAC expects there will be consistently new information available as the COVID-19 pandemic evolves.

"PRIVACY" MEANS PRIVACY OF "PERSONAL INFORMATION", BROADLY DEFINED

374. "Classically understood as the right to be left alone, the concept of privacy in today's high-tech world has taken on many new dimensions."[828] For this reason, there are many typologies of privacy[829], including privacy of *personal information and communication (unmediated and mediated)* – often referred to as "informational privacy"[830] – which is the primary focus of privacy protection laws in Canada[831].

375. "Personal information", including in digital format ("personal data"), is defined very broadly under Canadian privacy statutes (see details below) as "information about an identifiable individual"[832] (e.g., PIPEDA, subs. 2[1] and Privacy Act s. 3). PIAC has long argued that this expansive definition should not be confused with the much narrower and privacy-limiting concept of "personally identifiable information (PII)" which is an American concept that has no place in Canadian law. According to Osler, Hoskin & Harcourt LLP: "Generally,

information will be deemed to be about an 'identifiable individual' where it is reasonably possible for an individual to be identified through the use of that information, alone or in combination with other available information."[833] However, it is increasingly hard to know whether information held by entity X could be used to identify an individual when combined with information held by entity Y or available on the Internet, meaning that "more information may qualify for protection as 'personal information,' even though it does not directly identify an individual on its own".[834] For this reason, the historical distinction between "personal data" and "population-level, anonymous data" is increasingly blurry.

376. Types of personal information include: telephone number (landline and cell), home address, email address and messages, Internet protocol ("IP") address; birth date, age, height, weight, blood type, DNA code, fingerprints, voiceprint, health status (COVID-19 positivity); race/colour, national/ethnic origin, religion, marital status; medical, criminal, and employment records; income, financial transactions (purchases, spending habits, banking information, credit/debit card data, loan/credit reports), tax returns; social insurance number ("SIN"), driver's licence, other identification numbers; activities (online and offline); personal opinions; photos and contact lists; location data (because it can reveal user activity patterns); and metadata.[835]

377. Canadian law has taken an expansive approach to interpreting certain personal information available on mobile devices and the Internet. For example, according to the Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps:

> *"Whatever method is used to link a device to its owner, whether it's a unique device identifier or multiple linked identifiers, it has the potential to combine with personal information to create a profoundly detailed and sensitive profile of a user's behaviour depending on the circumstances. Combining disparate bits of information, derived from multiple sources, can also lead to detailed profiles that enable individuals to be identified. The Federal Court has ruled that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."*[836]

The Privacy Commissioner of Canada, in one investigation involving an ISP's use of deep packet inspection technologies, "held that that the IP addresses collected by the ISP were personal information even though they were not linked to individuals, because the ISP had the ability to make such a link".[837] The Commissioner has taken a similar approach to online behavioural advertising ("OBA"), holding that "much of the information used to track and target individuals with interest-based advertisements online – including such things as IP addresses, browser settings, internet behaviour – is personal information even where individuals are not personally identified".[838]

378. As noted, there are specific categories of personal information, including "personal health information", which is defined in PIPEDA in a very detailed but expansive manner that covers all aspects of testing, treatment and follow-up, including, PIAC submits, any controls related to these clinical steps, including public health controls such as contact tracing, isolation and quarantine:

> ***personal health information,*** *with respect to an individual, whether living or deceased, means*
>
> *(a) information concerning the physical or mental health of the individual;*
>
> *(b) information concerning any health service provided to the individual;*
>
> *(c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;*
>
> *(d) information that is collected in the course of providing health services to the individual; or*
>
> *(e) information that is collected incidentally to the provision of health services to the individual.*[839]

Personal health data is always regarded as "sensitive" under PIPEDA and therefore attracts requirements of explicit consent to any collection, use, or disclosure (see details below).

LEGAL FRAMEWORK FOR PROTECTING PERSONAL INFORMATION ("PRIVACY LAW") GOVERNS ITS COLLECTION, USE & DISCLOSURE

379. The Canadian legal framework for protecting personal information ("privacy law" or "data protection law"[840]) fundamentally protects personal information by governing its collection, use, and disclosure ("sharing"). Sensitive personal data, such as health data, generally has more stringent protections.

PRIVACY LAW IS QUASI-CONSTITUTIONAL & RECOGNIZES NEED TO BALANCE OTHER INTERESTS (e.g., PUBLIC HEALTH-SAFETY)

380. "The right to privacy is an internationally recognized right".[841] However, Canada does not have an explicit right to privacy, meaning the word "privacy" does not appear in its constitution, specifically in the *Canadian Charter of Rights and Freedoms*[842] ("Charter").[843] Instead, Canada has: "construed a general right to privacy from other rights in (its) constitutional catalog (…) connected most strongly to the protection against unreasonable search and seizure or the right to make certain fundamental choices without the interference of government, but also (…) anchor(ed) in other constitutional rights (…)".[844] Other constitutional rights include the right to freedom of belief and expression, the right against self-incrimination, and right to life, liberty, and security of the person.[845] Consequently, Canadian privacy law is accurately described as "quasi-constitutional".[846]

381. The quasi-constitutional status of Canadian privacy law contrasts with the explicitly rights-based approach to privacy taken by other jurisdictions with heightened legal privacy protections, such as the EU pursuant to the GDPR.[847]

382. Canadian privacy law "(has) always recognized the need for balancing of interests. Privacy, as a moral or legal principle, does not trump all other laws or interests"[848], including public health and safety. PIAC's view on finding the *proper* balance between privacy and public-health-safety in the specific context of DCTT related to COVID-19 and future pandemics is detailed above.

PRIVACY LAW HAS MYRIAD SOURCES & COMPETENT AUTHORITIES

383. Canadian privacy law has myriad sources – a mix of statutes, regulations, and common law – and competent authorities, including the following.

PRIVACY STATUTES & PRIVACY COMMISSIONERS

384. **Canadian privacy statutes (overall).** The "paramount issue for privacy legislation" is "setting boundaries for how covered entities can collect, use, and share personal information".[849] There are Canadian statutes *specifically aimed at protecting personal information*, at the federal and PT level (including municipal)[850] ("Canadian privacy statutes" or "Canadian privacy legislation"), governing personal information that is held by:

- *government institutions* (aka "public bodies") ("public sector privacy legislation")[851];
- *private organizations engaged in commercial activities* (aka "businesses" or "enterprises") ("private sector privacy legislation")[852]; and
- *health information custodians*, public and private, in context of providing healthcare services ("health privacy legislation")[853].

385. **Summary of Canadian privacy statutes.** A high-level summary of FPT privacy legislation and its potential application to COVID Alert Canada and Ontario is provided in the following table (see details below and in Appendix B), which reveals that what statute(s) applies depends on the nature of the entity involved and the type of personal information:

Type of Entity	Type of Data	Federal Statute	PT Statute
Government (federal/PT)	Personal	Privacy Act (federal)	Public sector privacy act (PT)
Business (federal/PT)	Personal	PIPEDA (federal or *PT) *unless GiC Exemption Order re: *intra-provincial* collection/use/disclosure (i.e., AB, BC, QC – see next column)	Private sector privacy act (if PT) (AB, BC, QC have legislation "substantially similar" to PIPEDA)
"Health custodian" or "agent" thereof (PT only – government or business)	PHI	N/A (if PT government) PIPEDA (if PT business) unless GiC Exemption Order re: *intra-provincial* collection/use/disclosure (i.e., ON, NB, Nfld + LD, NS – see next column)	Health sector privacy act (ON, NB, Nfld + LD, NS have legislation "substantially similar" to PIPEDA)
	Non-PHI personal	N/A (if PT government) PIPEDA (if PT business) – see above	Public sector privacy act (if PT government) Private sector privacy act (if PT business)

386. **PT *private sector* privacy statutes**. Some PTs have private sector privacy legislation. The Governor in Council of Canada ("GiC") may, where satisfied that PT legislation is "substantially similar" to PIPEDA, Part 1 (pursuant to Industry Canada's test) exempt entities (other than federally-regulated businesses) from its application to collecting, using, and disclosing personal information *within the PT*.[854] The only PTs with private sector privacy statutes deemed substantially similar to PIPEDA are Alberta, British Columbia, and Quebec.[855] Lawyer Carole Piosevan emphasizes that: "It is still possible for an organisation to be subject to more than one privacy law, such that one part of its operations taking place within the province is governed by provincial law and another part of its operations – which might involve the transfer of information across provincial borders – is subject to PIPEDA."[856]

387. **PT *health* privacy statutes.** For purposes of PT versions of COVID Alert Canada, PT health privacy legislation (where it exists) applies to "health information custodians" ("custodians"), *whether or not in the course of business*, and entities that act on their behalf ("agents"), that collect, use, and disclose "personal health information (PHI)".[857] It follows that if PHAs or any other entity involved with the app qualify as "custodians" or "agents", they are covered by the relevant Acts. GiC may declare that PT privacy health statutes are "substantially similar" to PIPEDA[858], thereby exempting entities from its application to collecting, using, and disclosing PHI *within the PT*.[859]

388. In Ontario, the relevant health privacy legislation is the *Personal Health Information Protection Act, 2004* ("PHIPA"). GiC has declared, by way of an order, that PHIPA is "substantially similar" to PIPEDA, Part 1, therefore health information custodians (and their agents) are exempt from the application of PIPEDA, Part 1, *to the extent they collect, use, and disclose PHI within Ontario,* and must comply with PHIPA. [860] Ontario health information custodians and their agents that *in the course of commercial activities* collect, use, and disclose PHI outside Ontario – say, to GoC or other PTs – must *also* comply with PIPEDA Part 1. Additionally, all personal information *that is not PHI* continues to be governed by PIPEDA.[861]

389. **Review of Canadian privacy statutes.** Federal privacy statutes, namely the Privacy Act (public sector) and PIPEDA (private sector), are subject to ongoing review by GoC (see details below). Some PT privacy statutes are also subject to ongoing review (e.g., pursuant to Ontario's public consultation "to strengthen privacy protections of personal data"), proposed modernization (e.g., Quebec's bill for *An Act to Modernise*

Legislative Provisions as Regards the Protection of Personal Information, proposing amendments to public and private sector privacy laws), and during-pandemic revisions (e.g., March 2020 revisions to Ontario's PHIPA[862]) (see details below).

390. **Canadian privacy commissioners.** Canadian privacy statutes are administered by independent privacy and/or access to information commissioners ("privacy commissioners" or "privacy regulators") in each jurisdiction, including OPCC at the federal level and, in Ontario, IPC. Privacy commissioners report to their respective legislatures and, in addition to overseeing the relevant privacy statutes, have the power to issue regulatory guidance ("guidance"), which is not legally binding, to help entities subject to privacy statutes understand their privacy-related obligations. Privacy commissioners have exercised this power – individually[863] and collectively – to issue guidance on privacy and COVID-19 ("COVID-19 privacy guidance"), including the following, in reverse chronological order (see details below and in Appendix B):

- May 2020 Joint OPCC-PT Privacy Commissioner Guidance to FPT governments ("May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance");
- April 2020 OPCC Guidance to GoC ("April 2020 OPCC COVID-19 Privacy Guidance"); and
- March 2020 OPCC Guidance to GoC & Businesses ("March 2020 OPCC COVID-19 Privacy Guidance").

Most privacy commissioners have the power to investigate and decide upon complaints from the public, albeit their findings may or may not be "enforceable", depending on the legislation.

391. **Right to privacy in Canadian privacy statutes.** Canadian privacy statutes do not formally recognize privacy as a right in and of itself but rather, according to OPCC, "are narrowly framed as data protection statutes" that "codify a set of rules" for how covered entities "are required to handle an individual's personal information" (aka "data protection principles" or "privacy principles").[864] Further, Canadian privacy statutes do not define the right to privacy in its broadest sense in accordance with Supreme Court of Canada ("SCC") jurisprudence, which effectively defines privacy as "an individual's rights to live and develop independently, free from unjustified surveillance, while still participating in the activities of a modern digital society."[865] Legal experts explain that:

> *"The SCC has recognized privacy to include a notion of anonymity – that one may act in public without being personally identified or subject to extensive surveillance. Recently, the SCC concluded that privacy is not an "all-or-nothing" concept and that being in a public place does not negate all expectations of privacy with respect to being observed or recorded. The SCC has also held that privacy is vital to an individual's dignity, autonomy and personal growth, and thus that protection of privacy is a prerequisite to a free and healthy democracy."* [866]

OPCC has recommended modernizing federal privacy statutes in ways that include adopting a privacy rights-based approach and defining the right to privacy broadly, to align with SCC jurisprudence and recognize the quasi-constitutional nature of privacy laws[867] (see details below).

392. **Comparison of Canadian privacy statutes.** Canadian privacy statutes have similarities and differences:

> *"While there are some similarities between privacy laws across the country, there are also key differences. This includes differences in the standards for obtaining consents from individuals and the types of exemptions federal and provincial authorities and private organizations might look for. There is not, for example, a common framework like there is in the European Union under the GDPR which contains specific exemptions for processing data including when processing is necessary for reasons of substantial public interest and specific exemptions for health data."*[868]

Notwithstanding these differences, it is possible to identify key privacy terms, privacy principles, and rights that individuals have in relation to the processing of their personal data ("individual rights") (collectively, "privacy protections")[869] (see details below).

SECTOR-SPECIFIC STATUTES WITH PRIVACY PROVISIONS: TELECOMMUNICATIONS ACT & CRTC

393. There is sector-specific legislation that contains privacy provisions. A key example is the federal *Telecommunications Act*[870], ("Telecommunications Act" or "Telecom Act") which contains privacy provisions that apply to TSPs, administered by CRTC .

394. PIAC's position is that FPT privacy commissioners have limited jurisdiction over TSPs, at their respective levels, pursuant to PIPEDA[871], and that CRTC:

- is the only regulator with plenary jurisdiction and enforcement power to allow or prohibit use of confidential customer information obtained from Canadians' use of their TSPs' services or any other aspect of telecommunications , pursuant to the *Telecommunications Act*; and
- has stated in some of its decisions (e.g., Telecom Decision 2003-33) that its jurisdiction over privacy of telecommunications is *separate and additional* to privacy commissioners' jurisdiction under PIPEDA[872].

395. We note that, prior to the Application filed with the CRTC today, PIAC previously has attempted to involve CRTC in network-level COVID-19 contact tracing, by way of an application dated May 4, 2020[873] ("May 2020 PIAC Part 1 Application on Contact Tracing") requesting Commission action to ensure that pandemic contact tracing applications for public health purposes are developed "in the fairest, most open and transparent manner, non-coercively and only for the intended purpose(s)". Our application was formally rejected by CRTC via a letter decision dated August 17, 2020.[874] Should OPCC identify network access of any COVID-19 contact tracing applications, we urge OPCC to communicate with CRTC in an effort to convince CRTC to investigate the network aspects of any app that may violate privacy under PIPEDA, the Privacy Act or the Telecom Act. On the Telecom Act potential violations, please see the text of the May 2020 PIAC Part 1 Application on Contact Tracing. This recommendation is revisited below.

PRIVACY TORTS, OTHER PROTECTIONS & COURTS

396. Privacy interests are legally protected in other ways, including: statutory and common law torts of invasion of privacy ("privacy torts"); *Criminal Code*[875] offences (e.g., voyeurism); and *Quebec Charter of Human Rights and Freedoms*[876] ("Quebec Charter") and *Civil Code of Quebec*[877] provisions protecting privacy rights.[878] These privacy protections are generally administered by courts.

EXCEPTIONS TO PRIVACY PROTECTIONS FOR EMERGENCY OR PUBLIC HEALTH CRISIS ("PRIVACY EXCEPTIONS")

397. There are legal exceptions to privacy protections ("exceptions to privacy protections"). Generally, these exceptions are narrow and circumscribed.

398. **Exceptions in Canadian privacy statutes (FPT).** Exceptions to privacy protections exist in Canadian privacy statutes. These provisions permit personal information to be collected, used, or disclosed for specific reasons that may be relevant in the context of an emergency or public health crisis, or when the public interest otherwise trumps the protection of privacy.[879] The text of these exceptions must be reviewed carefully to assess their application (aka "leveraging" by government institutions, health custodians, and businesses) in a specific situation, such as COVID-19.[880]

399. **Exceptions in public health protection legislation (FPT).** Exceptions to privacy protections also exist in public health protection legislation, both federal and PT, such as:

- Federal: *Quarantine Act*[881], which establishes a duty to disclose personal data to border-screening officials where there are reasonable grounds to believe a person has been exposed to a communicable disease.[882]
- PT: Ontario's *Health Protection and Promotion Act*[883], which permits designation of a "reportable communicable and virulent disease", creating the duty to disclose it (used for SARS in 2003); and Quebec's *Public Health Act*[884], which permits the director of public health to issue an order to "do

everything reasonably possible" to find and apprehend a person where there is "a real threat to the health of the population".[885] In some PTs (e.g., Northwest Territories), the Chief Public Health Officer "has broad powers to collect, use and disclose personal information to protect public health, whether or not a formal health emergency is declared".[886]

400. **Exceptions in Emergency Orders (FPT).** Emergency orders can create particular (often time-limited) exceptions to privacy protections in context of a specific public or general emergency:

> *"Where there is a declaration of public emergency, powers to collect, use, and disclose personal information may be expanded, within the bounds of the specific law in question. Privacy Commissioners across Canada have highlighted that the principles of necessity and proportionality should inform decisions made to address the current (COVID-19) crisis."*[887]

As noted, FPT privacy commissioners have also emphasized that, in the COVID-19 context, "(n)ormal privacy laws apply unless emergency legislation provides otherwise"[888] (see details below).

401. Emergency orders pertaining to COVID-19 have been issued. For example, whereas GoC did not invoke the *Emergencies Act* to declare a "public health emergency" to address the pandemic[889], on March 25, 2020, Canada's Minister of Health announced a COVID-19 Emergency Order under the *Quarantine Act*, making it possible existing exceptions in federal privacy statutes will be relied upon.[890] On June 30, 2020, GoC extended the Emergency Order requirements related to isolation and quarantine until August 31, 2020, for travellers entering Canada.[891] Certain PT governments (e.g., BC, Ontario, and Quebec) have also issued COVID-19 emergency orders[892], of which some include expanded powers over personal data (e.g., Ontario – see details below). To date, no government – federal or PT – has invoked emergency management legislative powers to by-pass or use alternate authority for *contact tracing*.

402. Ontario's state of emergency – declared on March 17, 2020 in Order in Council 518/2020 (Ontario Regulation 50/20), pursuant to the *Emergency Management and Civil Protection Act* ("EMCPA") – was extended to July 24, 2020[893] and all in-force emergency orders made thereunder were extended to July 29, 2020[894]. The Solicitor General clarified that:

> *"As per the (EMCPA), following the termination of a declaration of emergency, emergency orders can be extended, but not amended, if they are necessary to deal with the effects of the emergency. We are taking the time to carefully review all emergency orders issued and determine the best next steps, should the declaration of emergency terminate. This may include extending an order, terminating an order, or introducing legislative or regulatory changes in place of an order. As per the Health Protection and Promotion Act, local Medical Officers of Health maintain their powers under Section 22 regardless of a declared state of emergency."*[895]

Pertinent Ontario emergency orders include: Ontario Regulation O. Reg. 120/20[896] for "access to COVID-19 status information by specified persons" that permits the sharing of COVID-19 infection status information with first responders, including law enforcement, for the purpose of their protection[897]; and Ontario Regulation O. Reg. 190/20[898] for "access to personal health information by means of the electronic health record", permitting use of the record to collect personal health information by medical officers of health, certain registered nurses, and coroners, and granting Ontario Health power to make public health information available by means of the record to the foregoing entities "even if Ontario Health does not have custody or control of" it.

403. Effective July 24, 2020, according to the Ontario government:

> *"Ontario has transitioned into the recovery phase with the new Reopening Ontario (A Flexible Response to COVID-19) Act. While the provincial declaration of emergency has ended, the new act will provide the province with the necessary flexibility to address the ongoing risks and effects of the COVID-19 outbreak. Some emergency orders that were previously in place under the Emergency Management and Civil Protection Act, will continue under the new act. This*

includes orders related to labour redeployment in long-term care and retirement homes, stages of reopening, compliance with public health advice and gatherings."[899]

Emergency order O. Reg. 190/20 also remains in force, however O. Reg. 120/20 is revoked.[900] Prior to the revocation of O. Reg. 120/20, it was the subject of a legal challenge by the CCLA et al. to end police access to the COVID testing results database. Data released by the province showed that Ontario police services searched the COVID database 96,815 times from April 17-July 20, 2020.[901]

404. **Exceptions in privacy commissioner guidance (FPT).** Additionally, privacy commissioners' guidance on privacy in context of a particular pandemic can "highlight" (not grant) exceptions to privacy protections.[902] This is true for privacy commissioners' COVID-19 privacy guidance, including:

- the May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance, April 2020 OPCC COVID-19 Privacy Guidance, and March 2020 OPCC COVID-19 Privacy Guidance (see details above and below); and
- individual PT privacy commissioner guidance that highlights the exceptions in provincial privacy statutes, including by[903]:
  - Ontario (March 2020, updated June 2020[904] - pertaining to privacy commissioner's operations and "tips" for working at home but not how to interpret Ontario's privacy legislation during COVID-19); and
  - Alberta (March 2020[905]); BC (March 2020[906]); Manitoba (date unknown[907]); New Brunswick (March 2020[908]); Newfoundland and Labrador (April 2020[909]); Northwest Territories (March 2020[910]); Nova Scotia (March 2020[911]); Quebec (March 2020[912]); Saskatchewan (April 2020[913]); and Yukon (March 2020[914]).

405. **Exceptions in international agreements.** Finally, international agreements between Canada and other countries can grant exceptions to Canadian privacy protections, such as restrictions on the transfer of personal data to other jurisdictions (see details below). For example, in a June 2019 meeting, Canada's Attorney General David Lametti and US counterpart William Barr discussed a controversial law, the *Clarifying Lawful Overseas Use of Data ("CLOUD") Act* that allows police to get faster access to data stored in other countries.[915] As of June 2020, neither government would confirm whether they are negotiating a bilateral agreement, however the US has struck such a deal with the UK and Australia.[916] Lawyers and civil liberties groups warn a Canada-US agreement could undermine domestic privacy protections, and OPCC said its support would be conditional on the agreement's provision of explicit safeguards and maintained court oversight (e.g., judicial authorization of warrants and information production orders).[917]

PRIVACY PROTECTIONS/EXCEPTIONS FURTHER COMPLICATED BY SILOED APPROACH TO CANADIAN PUBLIC HEALTH POLICY

406. In Canada, privacy protections are further complicated by the siloed approach to public health policy, overall and regarding COVID-19, especially in Ontario.

407. **Siloed approach to health policy overall.** Overall, as noted, roles and responsibilities for public health and health-care are shared between GoC and PT governments.

408. **Siloed approach to COVID-19 health policy.** Official COVID-19 pandemic preparations by FPT governments and PHAs were "mounted not as one country, but in silos" as "(e)ach province charted its own course", reflecting "wider dysfunction within the Canadian health care system".[918] For example:

- Health ministries and agencies:[919] As noted, Canada has a Minister of Health, supported by Health Canada and PHAC, which is tasked with protecting Canada from serious public health threats. However, on March 4, 2020, Deputy PM Chrystia Freeland assumed control of the COVID-19 file. Each PT has its own health ministry (e.g., Ontario's Ministry of Health) and agency (e.g., Public Health Ontario ["PHO"]).

- Chief medical officers:[920] Canada has a Chief Public Health Officer (Theresa Tam) and each PT has its own chief medical officer (e.g., Ontario's Chief Medical Officer of Health ["CMOH"] David Williams).
- Laboratories:[921] Canada has a National Microbiology Lab ("NML") (under PHAC), and each PT has its own labs, both public health, commercial, and hospital. Ontario laboratories (unlike BC, Alberta, and Quebec's) are not integrated, meaning public health labs, commercial labs, and hospital labs all report to different part of the provincial health ministry.
- Testing guidelines:[922] Testing criteria for COVID-19 ("testing guidelines") are issued by GoC and individual PTs, and sometimes conflict.

409. **Ontario's siloed approach.** Ontario's health care system is especially complex, because it is not centralised or integrated and thus has an unclear chain of command. This complexity has negatively impacted Ontario's response to COVID-19:

> *"The structure of Ontario's health care system exacerbated tensions. For COVID-19, there were five big players: the Chief Medical Officer, the Ministry of Health, the Ministry of Long-Term Care and then two agencies, Public Health Ontario – which is the equivalent to the BCCDC – and Ontario Health, a new entity that was supposed to try to co-ordinate the province's disparate system. That work got going in earnest just before the outbreak. On top of all that, there are 34 public health units and then all the hospitals.*
>
> *By contrast, Alberta's health care system – including the hospitals – are all under one umbrella, which Geoffrey Taylor, the Senior Medical Director of Infection Prevention and Control with Alberta Health Services, says was a huge asset. "Sometimes an integrated system can have drawbacks, [but during a pandemic] it's an advantage," Dr. Taylor said.*
>
> *Quebec and B.C.'s health care systems are also more centralized. In Quebec, there are 18 health regions, but they are co-ordinated by the ministry. B.C. has five health authorities, but even though they operationally report to a local board, they too report to the ministry, which directs policy. Many of the province's top infectious-disease experts are connected to the BCCDC, which reports to the provincial health officer, Dr. Henry. It was always clear that Dr. Henry was steering the response in B.C.*
>
> *In Ontario, the chain of command was unclear to the experts, meaning when problems arose they weren't even sure where to direct complaints(…)*
>
> *'I do think it's been challenging. It's been hard to know what tables are responsible for certain decisions. There's a lot of overlap,' said Susy Hota, the Medical Director of infection Prevention and Control at University Health Network in Toronto(…)*
>
> *In an interview, Ontario's Chief Medical Officer David Williams acknowledged that the structure of the province's health system presents communication challenges. For example, public health units are managed by local municipal boards. 'While I work with them, they do not report to me,' he said."*[923]

410. This siloed approach to Canadian public health policy, overall and regarding COVID-19, especially in Ontario, complicates the task of determining how the data flow works for any given personal information-gathering initiative (manual or digital).

HEART OF PRIVACY LAW IS PRIVACY PROTECTIONS

411. The heart of privacy law is privacy protections, specifically privacy principles and individual rights, which are outlined at a very high level here.

412. First, however, it is important to identify key privacy terms. As noted, privacy law protects the use, collection, and disclosure of personal data. A working definition of these and associated terms pursuant to Canadian privacy statutes is helpful, especially for international comparison purposes:

- "Processing": Generally, not expressly defined under Canadian privacy statutes. In practice, processing includes collecting, using, modifying, storing, disclosing, or destroying personal data.[924]
- "Processor" and "controller": Generally, not expressly defined under Canadian privacy statutes, which refer to "organizations" more broadly (including processors and controllers).[925]
- "Data subject": Generally, not expressly defined under Canadian privacy statutes, which refer to "individuals".[926]
- "Data breach": Generally, not expressly defined under Canadian privacy statutes. However, some refer to "breach of security safeguards"[927] or a similar term, effectively defined as *loss of, unauthorized access to, or unauthorized disclosure of* personal data resulting from a breach of an organization's safeguards or failure to establish those safeguards.[928]
- "Sensitive personal data": Generally, not expressly defined under Canadian privacy statutes.[929] PIPEDA provides that "any information can be sensitive, depending on the context"[930] and, as noted, personal health data is always regarded as "sensitive" thereunder[931].

PRIVACY PRINCIPLES

413. Following are the key privacy principles (and privacy exceptions) under Canadian privacy statutes (FPT), particularly *private* sector (hence "organisations" is synonymous with "businesses" and, by corollary, "government institutions" are excluded unless noted otherwise). A detailed overview of privacy principles specific to *federal privacy statutes, both private and public sector,* is provided in Appendix B.

414. **Transparency/openness.[932]** Organisations must document and make available information about their policies and practises related to managing personal data.

415. **Lawful basis for processing (consent).[933]** Organisations must *obtain consent* to collect, use, and disclose personal data, subject to limited exceptions. Consent must be:

- *valid* (reasonable expectation that nature, purpose, and consequences are understood);
- limited to fulfilling an explicitly specified and legitimate *purpose*;
- obtained by fair and lawful *means*;
- in a *form* (express or implied) that depends on the data's nature and individuals' reasonable expectations (as noted, under PIPEDA, personal health data is always regarded as "sensitive" and therefore attracts requirements of explicit consent to any collection, use, or disclosure[934]); and
- capable of *withdrawal* at any time (subject to legal or contractual restrictions and reasonable notice). Upon withdrawal, organisations must inform individuals of its implications.

416. **Purpose limitation.[935]** Organisations must identify *purpose(s)* for which personal data is *collected*, at or before the collection time, document such purposes in accordance with the transparency principle, and not use or disclose the data for other purposes except with consent or as required by law. See also data minimisation and proportionality principles.

417. **Data minimisation.[936]** Organisations must *collect, use, and disclose* personal data only to the extent (in type and volume), and *retain* it only as long as, necessary to fulfill the identified purpose(s).

418. **Proportionality.[937]** Organisations must only *collect, use, and disclose* personal data for *purposes* that reasonable individuals would consider appropriate in the circumstances. This principle is built into some of the others, such as the purpose limitation, safeguarding principle, and accuracy principle.

419. **Retention.**[938] Organisations must *retain* personal data only as long as necessary to fulfil the purpose(s) for which it was collected, except for valid legal requirements, *destroy, erase, or anonymize* it when it is no longer needed to fulfill the purpose(s), and *make guidelines and implement procedures* about retention (e.g., minimum/maximum retention periods and destruction processes). See also data minimisation principle.

420. **Accountability.**[939] Organisations must *protect ("safeguard")* personal data that is under their control – including when it is transferred to third parties for processing ("third-party processors"), at a comparable level of protection, through contractual or other means – designate a person to be accountable for the organisation's compliance with all privacy principles[940] (e.g., Chief Privacy Officer), and implement those principles in policies ("privacy policies") and practices ("privacy practices").

421. **Safeguarding.**[941] Organisations must *safeguard* personal data that is under their control – including data that is transferred to third-party processors (see above) – by implementing reasonable measures (technical, physical, and administrative) to protect it against loss, theft, and unauthorized access, copying, use, disclosure, change, or destruction. The more sensitive the data, the higher the level of protection required.

422. **Accuracy.**[942] Organisations must ensure personal data in their records is accurate, complete, and current, especially when it is used to make a decision about the individual or it is likely to be disclosed to a third party.

INDIVIDUAL RIGHTS

423. Following are the key individual rights under Canadian privacy statutes[943] (FPT), particularly *private* sector (hence "organisations" is synonymous with "businesses" and, by corollary, "government institutions" are excluded unless noted otherwise). These individual rights to personal data in the custody of covered entities: "recognize an essential element of privacy: that individuals retain interests in the personal information they share with others and that – rather than exercise absolute dominion over this information – the (entities) that receive it exercise shared control over (it)."[944]

424. **Right of access to data/copies of data.**[945] Organisations must, subject to limited exceptions[946], upon request, inform individuals of the *existence, use, and disclosure* of their personal data, give them *access* to it, and *provide a list* of third parties it was shared with, within a prescribed time limit or reasonable period, at no or minimal cost, and in a generally understandable form.

425. **Right to rectification of errors.**[947] When individuals demonstrate their personal data is inaccurate or incomplete, organisations generally must correct it or add a notation.

426. **Right to deletion/right to be forgotten.**[948] There is no right to require organisations to "erase" or delete personal data. (However, as noted, there is an individual right to withdraw consent.)

427. **Right to object to, or restrict, processing.**[949] There is no right to object to, or restrict, processing of personal data. However, organisations are prohibited to require – as a condition for providing a product (good or service) – consent to collect, use, or disclose personal data beyond what is needed to fulfill the specified purpose.

428. **Right to data portability.**[950] There is no right to data portability.

429. **Right to withdraw consent.**[951] As noted, there is a right to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and individuals must be informed of the implications.

430. **Right to object to marketing.**[952] Consent is required to collect, use, or disclose personal data for *marketing purposes.* The required *form* of consent (opt-in or opt-out) depends on the circumstances, data sensitivity, and reasonable expectations of the individual. If opt-out, conditions must be met (e.g., make individual aware of marketing purposes at or before time of collection, opt-out that is easy, immediately effective and persistent, and asap destruction or de-identification of data collected and used). Electronic direct marketing

(e.g., email or SMS) is also subject to requirements under Canada's anti-spam legislation ("CASL") (enforced by CRTC) whereas telephone marketing is also subject to CRTC's *Unsolicited Telecommunications Rules*, which include requirements related to the National Do-Not-Call List ("National DNCL").

431. **Right to complain to relevant data protection authority(ies).**[953] There is a right to complain to the relevant data authority and, prior to this, to the organisation's designated person with accountability for its privacy compliance. Organisations must have easy-access and simple-use procedures to respond to complaints and take steps to effectively address them.

KEY PRIVACY ISSUES: PRIVACY IMPACT ASSESSMENT ("PIA"), EMPLOYEE MONITORING & INTERNATIONAL DATA TRANSFER

432. Privacy issues that are pertinent to DCTT and related digital health technology include registration/notification or prior approval by privacy commissioners of processing activities, privacy impact assessment, employee monitoring, and international transfers of personal data. This section focuses on *private* sector privacy statutes (FPT) (thus "organisations" is synonymous with "businesses" and, by corollary, "government institutions" are excluded unless noted otherwise).

433. **Registration/notification or prior approval of processing activities:** Canadian privacy statutes generally do not require organisations to register with, or notify, privacy commissioners in respect of personal data processing activities.[954] The exception is organisations that want to use or disclose data *without consent* for *statistical, scholarly study, or research purposes* must notify OPCC prior to doing so.[955]

434. **Privacy Impact Assessment ("PIA").** A Privacy Impact Assessment ("PIA") is an evaluation process that enables an entity to assess and evaluate the privacy, confidentiality, or security risks associated with the collection, use, or disclosure of personal data, and to develop measures to eliminate (wherever possible) or mitigate those risks.[956] Any Canadian *government* initiative that uses personal data is mandated (federally, through a Treasury Board of Canada Secretariat Directive[957] ["TBS Directive"]), or expected, to be subject to a PIA[958], however no prior approval (i.e., submission prior to deployment) is required. The proviso is that the TBS Directive is replaced with an "Interim Directive on Privacy Impact Assessment"[959] for the period March 13, 2020 to September 30, 2020 that sets out, in section 6.4, "requirements for an urgent COVID-19-related initiative". The requirements relate to PIAs (discretion to complete a "Privacy Compliance Evaluation" for a new or substantially modified program instead of a full PIA) and registration of new or modified Personal Information Banks (discretion to defer the submission of the registration request). Some PIAs are published, generally on a voluntary rather than mandated basis. "Best practice" is to submit the PIA to privacy commissioners for review, amend it according to their recommendations, and get it approved when privacy compliance is established.[960] From PIAC's perspective, the primary function of PIAs is to demonstrate due diligence (not, as is often claimed, for transparency and accountability to Canadians) and they are no substitute for compliance and enforcement, audits, or complaints.

435. **Employee monitoring.**[961] Workplace privacy is a complicated, contentious, and controversial area, due to competing interests: "employees wish to have their privacy rights respected and protected" whereas "employers want to ensure that activity in the workplace does not negatively impact their business".[962] Employee monitoring, within and outside the private sector workplace, is permissible if it complies with: the privacy principles under Canadian privacy statutes; workplace health and safety legislation; labour relations legislation and rulings; particular workplace agreements (collective agreements and arbitrations); and human rights and constitutional law (Charter). In particular:

> *"(T)he monitoring must be conducted for a purpose consistent with what a reasonable person would consider appropriate in the circumstances. Canadian privacy regulatory authorities generally use a four-part test to assist in determining the reasonableness of employee monitoring:*
>
> - *Is the surveillance demonstrably necessary to meet a specific need?*
> - *Is the measure likely to be effective in meeting that need?*

- *Is the loss of privacy proportional to the benefit gained?*
- *Is there a less privacy-invasive way that the employer could achieve the same end?"*[963]

The statutes allow for personal data of employees to be collected, used, and disclosed without consent, within the bounds of reasonableness (i.e., for purpose of creating, managing, or ending an employment relationship), provided employers are transparent (i.e., provide notice and reasons, such as employee health-safety).[964]

436. **International data transfers**. Finally, Canadian privacy statutes include provisions on the transfer of personal data to other jurisdictions (e.g., to an out-of-Canada, third-party data processor ["foreign processor"]). Generally, the statutes permit non-consensual transfer of personal data to third-party data processors in other countries, using contractual or other means, provided the transferring organisation provides a comparable level of protection to that under the statutes:

> *"Typically, companies enter into an agreement when transferring data outside of Canada for processing purposes to ensure that the data transferred is afforded a comparable level of protection to that under Canadian Privacy Statutes. Depending on the size and the context of the data transfer arrangement in question, there are a number of measures that companies take to establish an appropriate vendor management framework, including: (i) due diligence, in particular with respect to security safeguards; (ii) contractual arrangements setting out requisite controls and conditions; (iii) appropriate notice to employees or consumers; and (iv) appropriate monitoring of the service provider arrangement. <u>While consent per se is not required, notification is</u>."*[965]

However, this a highly contentious and complicated area. For example, OPCC at one time permitted complaints about non-consensual international data transfers *despite notice*, but it has since retreated on this position. Further, these domestic rules sometimes bump up against international agreements (see details above).

CONCLUSION: DCTT IS SUBJECT TO MYRIAD, COMPLEX, OVERLAPPING, & INCONSISTENT CANADIAN PRIVACY LAWS

437. The foregoing discussion demonstrates that during a public health crisis such as the COVID-19 pandemic, which involves close coordination between different levels of government, many layers of Canadian privacy law and administrators play a concurrent, intersecting, and sometimes conflicting role. It follows that DCTT and related digital health technology is subject to:

- myriad, complex, overlapping, and inconsistent FPT privacy laws; and
- multiple privacy regulators, with potentially multiple and overlapping investigations and enforcement proceedings for privacy violations.

438. Further, the only way to determine what FPT privacy law(s) apply to a given DCTT or related digital health technology is to conduct a comprehensive data flow analysis that identifies all of the entities collecting, using, and disclosing personal information and their respective roles and responsibilities. This task is especially difficult due to the siloed approach to Canadian public health policy, overall and regarding COVID-19, especially in Ontario. It is further complicated in the case of DCTT owned/operated by GoC, in light of OPCC's recent emphasis on "the federal government's publicly stated goal of moving towards a 'tell us once' service delivery model, where data entered in one government system can be reused by multiple other government systems".[966]

COVID-19 HIGHLIGHTS GAPS IN CANADIAN PRIVACY PROTECTIONS PERTAINING TO DIGITAL TECHNOLOGIES ("DIGITAL PRIVACY GAP"), ACCELERATING NEED FOR PRIVACY LAW REFORM

439. Existing Canadian privacy laws, specifically privacy statutes, are outdated and do not effectively protect Canadians in the age of digital technology. In other words, there is a "gap in privacy protections" pertaining to digital technology ("digital privacy gap"). This digital privacy gap is *highlighted by* COVID-19, especially by DCTT.

440. **PIAC recommends that to fill the digital privacy gap, existing Canadian privacy legislation (FPT) must, on an urgent basis, be *modernized and strengthened*, ideally by aligning it with the GDPR. However, it is crucial to ensure that updated legislation "does not only focus on today's technologies but also what is on the horizon" (e.g., emerging digital technologies like blockchain), so that Canada can "foster the next wave of digital innovation while still protecting and empowering Canadians' data rights".[967]**

THERE IS A DIGITAL PRIVACY GAP, DRIVING NEED FOR STATUTORY REFORM

441. There is a digital privacy gap, and it drives the need for reform of Canadian privacy legislation (FPT).

THERE IS A DIGITAL PRIVACY GAP

442. "Canada's current privacy laws are antiquated and inadequate"[968] in that the legislative framework for privacy has not "kept pace" with digital technology, meaning it is not protecting Canadians from privacy violations that result from digital technology (e.g., data breaches, identity theft, surveillance, and commercial data brokerage) and "lead to loss of freedom, democracy, equality and even physical security"[969]. As such, the legislative framework is not designed for a digital economy where "personal information has become a primary currency" and "the stockpiling of personal information is increasingly seen as a competitive advantage".[970] This is a problem, not only for its own sake, but because poor privacy protection undermines Canadians' trust in digital technology, which is needed to grow said digital economy.

443. Whereas "Canada used to be a leader in privacy protection", now "the world is passing us by".[971] In particular, "(a)s Canadian law stagnates, European privacy rules have steadily advanced" pursuant to the 2018 GDPR, which could jeopardize the "adequacy" decision Canadian law has received from the European Commission[972], thereby leading to restrictions on EU-Canada data transfers[973]. Many other countries and jurisdictions have updated their statutory privacy frameworks to align with the GDPR, which "significantly strengthened privacy protections in the European Union by introducing more robust requirements for consent, transparency and enforcement, and provided individuals with greater control over their personal data".[974]

BRIDGING DIGITAL PRIVACY GAP REQUIRES MODERNIZING & STRENGTHENING PRIVACY LEGISLATION

444. There is general consensus that the digital privacy gap should be filled, by *modernizing and strengthening* Canadian privacy legislation, and the primary question is how. PIAC's nutshell position is that Canadian privacy legislation, at the federal and PT level, should be strengthened by adopting a rights-based approach to privacy and aligning statutory privacy principles with the GDPR.

445. Prior to the COVID-19 pandemic, the digital privacy gap and need to fill it by modernizing and strengthening privacy legislation was recognized by Canadian governments and privacy commissioners, particularly at the federal level. As of January 2020, according to Canadian Privacy Commissioner Therrien, "(t)he question is no longer whether (federal) privacy laws should be modernized, but how" and "the (federal) government has promised to act".[975]

446. **Federal legislative reform.** As noted, GoC review of the Privacy Act and PIPEDA is ongoing. In May 2019, Innovation, Science and Industry ("ISI") Minister Bains launched "Canada's Digital Charter: Trust in a Digital World" ("Digital Charter")[976] – which former Privacy Commissioner of Canada Jennifer Stoddart contends "clearly take(s) (its) cue from" the GDPR[977] – plus a set of actions to implement the Charter's ten principles[978] that include: confirmation of GOC's intent to modernize the Privacy Act ("Modernizing

Canada's Privacy Act"[979]); and GoC proposals to modernize PIPEDA ("Strengthening Privacy for the Digital Age"[980]):

> *"The proposal to modernize PIPEDA, Strengthening Privacy for the Digital Age, outlines a series of policy considerations related to specific proposals that would serve to enhance consumer control, enable responsible innovation and enhance enforcement. Specifically, the Government is proposing clarifications under PIPEDA that detail what information individuals should receive when they provide consent; certain exceptions to consent; data mobility; deletion and withdrawal of consent; incentives for certification, codes, standards, and data trusts; enhanced powers for the Office of the Privacy Commissioner; as well as certain modernizations to the structure of the law itself and various definitions. The Government is also studying potential reforms to the Privacy Act (…) and plans to engage expert stakeholders to ask for their views and feedback on technical and legal considerations."*[981]

447. The December 13, 2019, PM Trudeau mandate letters to ISI Minister Bains and Heritage Minister Steven Guilbeault[982] directs them to work with Justice Minister David Lametti to:

> *"advance Canada's Digital Charter and enhanced powers for the Privacy Commissioner, in order to establish a new set of online rights: data portability; the ability to withdraw, remove and erase basic personal data from a platform; the knowledge of how personal data is being used, including with a national advertising registry and the ability to withdraw consent for the sharing or sale of data; the ability to review and challenge the amount of personal data that a company or government has collected; proactive data security requirements; the ability to be informed when personal data is breached with appropriate compensation (…)"*[983]

Further, the letters direct the ISI Minister, with the Heritage Minister's support, to "create new regulations for large digital companies to better protect people's personal data", noting a "newly created Data Commissioner will oversee those regulations". Finally, the ISI Minister's mandate letter directs him to, with the Minister of Digital Government's support, "continue work on the ethical use of data and digital tools like artificial intelligence for better government".

448. As of June 5, 2020, GoC says it is working "to develop more concrete proposals for potential amendments to the (Privacy) Act"[984] . It is uncertain when a revised PIPEDA will be tabled, because the COVID-19 pandemic has disrupted the parliamentary schedule.[985]

449. OPCC has proposed specific changes to strengthen both the Privacy Act and PIPEDA. For example, A November 2019 letter from Privacy Commissioner Therrien to Heritage Minister Guilbeault calls for federal privacy laws to incorporate a "right-based framework… along with effective enforcement mechanisms" to "foster trust in government and business, giving individuals the confidence to fully participate in the digital age".[986] OPCC's "2018-2019 Annual Report" ("OPCC Annual Report"), tabled in December 2020, proposes changes to both federal acts.[987] The report also cites Facebook's "untenable" dismissal of OPCC's investigative findings that it had seriously breached Canadian privacy laws as evidence that "Canada requires updated privacy laws that provide for effective enforcement and recourse, and that consider privacy in its full spectrum of rights" to "help to restore trust in Canadian democracy and our economy".[988]

450. The OPCC Annual Report and GoC proposals on PIPEDA both "suggest reforms which aim to balance the economic opportunities enabled by the digital era with the associated risks to individuals' privacy rights" and are aligned on many issues (e.g., clarifying individuals' rights and business' obligations, enhancing individuals' control over personal information without creating onerous business restrictions, and enhancing enforcement).[989] Regardless of which proposals become law, the updates to PIPEDA "will force organizations doing business in Canada to take a proactive approach to privacy compliance and trigger comparable reforms to provincial (private sector) privacy legislation" because "a system in which federal and provincial privacy laws are not substantially similar is unworkable in the long term".[990]

INTERIM PRIVACY COMMISSIONER RESPONSE TO DIGITAL PRIVACY GAP IS GUIDANCE ON DIGITAL TECHNOLOGY

451. Pending legislative reform, FPT Privacy Commissioners have responded to the gap in Canadian privacy protections with privacy guidance on digital technology, in terms of over-arching issues (e.g., meaningful consent) and specific digital technologies or issues (e.g., mobile apps, location data, surveillance, etc.) (see details in Appendix B.

DIGITAL PRIVACY GAP IS HIGHLIGHTED BY COVID-19 (ESP. DCTT), ACCELERATING NEED FOR STATUTORY REFORM

452. The digital privacy gap is *highlighted* by COVID-19, particularly DCTT, and especially CTAs, accelerating the need for statutory reform.

COVID-19 (ESP. DCTT) HIGHLIGHTS DIGITAL PRIVACY GAP

453. According to OPCC, Opposition MPs, and privacy experts, the digital privacy gap is *highlighted* by COVID-19, particularly DCTT, and especially CTAs, accelerating the need for statutory reform. Illustrative examples follow.

454. **OPCC.** In a presentation prepared by OPCC ahead of an early May 2020 meeting, OPCC told Heritage Minister Guilbeault that COVID-19 has increased the need for privacy rights, for reasons including maintaining Canadians' trust in DCTT, and recommended the Privacy Act and PIPEDA should adopt a privacy rights-based approach and common privacy principles (due to increased public-private sector partnerships).[991] The OPCC briefing note prepared ahead of the meeting suggests that OPCC wondered how its work would intersect with the new Data Commissioner's work. [992] During a May 2020 House of Commons Industry, Science, and Technology ("INDU") Committee meeting, when Privacy Commissioner Therrien was asked if he was confident that Canadian privacy laws would protect Canadians against a CTA breach, he responded: 'No, I am not. My office has been talking for several years about the fact that our legal framework needs to be modernized and strengthened.'"[993] He also suggested that: "If we have a more robust legal framework, it is highly possible, virtually certain, that people would have more confidence in the system and would rely on these applications because they would see the benefits for public health. They would be less fearful of violations of their privacy".[994]

455. **Privacy experts.** At the same May 2020 INDU meeting, privacy experts expressed concerns. For example, Teresa Scassa "told MPs that the COVID-19 crisis had highlighted gaps in privacy law. 'COVID-19 is a wake up call in many respects. It's caught us with our privacy pants down, essentially,' she said. 'We need to have the digital legal infrastructure in place so that we can respond to situations as they come up. And we find ourselves in the situation with outdated privacy laws for the public sector and the private sector, and I think this is a disadvantage.'"[995] She had previously stated the "legal framework(…) is full of loopholes and question markets and uncertainties".[996] Michael Bryant, CCLA Executive Director, "told the committee that there were also concerns about use of the data, collected by contact tracing apps, by law enforcement agencies. 'Bottom lines would need to be set,' Bryant said, 'for example around data leakage to police and other investigation institutions or agencies. They should not be getting what amounts to public health data, under any circumstances'".[997]

456. **Opposition MPs.** On June 8, 2020, NDP MP Charlie Angus (Timmins - James Bay) sent a letter request to Privacy Commissioner Therrien regarding CTAs, asking for "elaborat(ion) on why simply following the current outdated legal privacy framework may still lead to misuse of Canadians' data". On July 29, 2020, certain Conservative MPs said they are concerned about privacy risks of COVID Alert Canada, for reasons including "that our existing privacy laws were not suited for this task" (aka "our privacy laws [are] inadequate").[998]

INTERIM PRIVACY COMMISSIONER RESPONSE TO PANDEMIC-HIGHLIGHTED GAP IS GUIDANCE ON COVID-19 (INCL. DCTT)

457. In response to the digital privacy gap related to the COVID-19 pandemic, as noted, FPT Privacy Commissioners, individually and jointly, issued COVID-specific guidance. In particular, OPCC, alone and together with PT privacy commissioners, issued guidance on privacy and the COVID-19 outbreak ("OPCC COVID-19 Guidelines" or "OPCC COVID-19 Privacy Guidance"), specifically (see details in Appendix B):

- May 2020 Joint OPCC-PT Privacy Commissioner Guidance to FPT governments entitled "Supporting public health, building public trust: Privacy principles for contact tracing and similar apps - Joint Statement by Federal, Provincial and Territorial Privacy Commissioners"[999] ("May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance" or "Privacy Commissioners' Joint Statement");
- April 2020 OPCC Guidance to GoC entitled "A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19"[1000] ("April 2020 OPCC COVID-19 Privacy Guidance"); and
- March 2020 OPCC Guidance to GoC & Businesses entitled "Privacy and the COVID-19 outbreak"[1001] ("March 2020 OPCC COVID-19 Privacy Guidance").

URGENT NEED FOR STATUTORY REFORM IS REINFORCED BY: PRIVACY COMMISSIONERS' ASSESSMENT OF COVID ALERT CANADA, PT PRIVACY LAW OVERHAULS & COURT DECISIONS ON PRIVACY (DOMESTIC & GLOBAL)

458. The urgent need for Canadian privacy legislation reform is reinforced by OPCC & IPC privacy assessments of COVID Alert Canada/Ontario, ongoing privacy law overhauls in Quebec and Ontario, and Canadian and EU court decisions on privacy.

459. **OPCC & IPC privacy assessments**. According to many experts, such as cybersecurity strategist and educator Claudiu Popa, the OPCC and Ontario Privacy Commissioner's assessment of COVID Alert Canada/Ontario "really makes it clear that Canadians are not well served by their current privacy legislation" and there is a "need for stronger legislative protections".[1002] The joint OPCC and IPC press release says the Health Canada Privacy Assessment suggesting the Privacy Act does not apply to COVID Alert Canada in light of Health Canada's assertion that the app does not collect "personal information" (whether or not it is legally valid) is a key reason to update federal privacy statutes:

> *"'(I)t bears noting that an app, described worldwide as extremely privacy sensitive and the subject of reasoned concern for the future of democratic values, is defended by the Government of Canada as not subject to its privacy laws,' the OPC's review report notes. 'This is again cause for modernizing our laws so that they effectively protect Canadian citizens.'"*[1003]

The OPCC assessment of COVID Alert Canada delves deeper, asking: "The design of this app is generally privacy sensitive, but does it mean it should be exempt from the law's purview? What legal remedies would citizens have if good design were to be inappropriately implemented?"[1004] Further, the OPCC assessment agrees with the Department of Justice's recommendation in its consultation papers on potential reform of the Privacy Act that:

> *"The current 'in or out' approach to personal information does not accommodate more nuanced rules that may be organized around different levels of risk and foster compliance. Defining de-identified, anonymized, and pseudonymized information could support the development of new compliance incentives, allow for a more targeted and nuanced application of certain rules, and assist to ease some of the difficulties of practical application that arise under the current approach."*[1005]

Finally, the OPCC assessment reiterates certain OPCC-proposed specific changes to the Privacy Act and PIPEDA (e.g., to "recognize that re-identification of personal information is always a possibility, depending on the context" and "define de-identified information to allow for a more targeted and nuanced application of certain rules").[1006]

460. **Quebec privacy law reform (Bill 64).** On June 12, 2020, the Quebec government tabled Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* ("Bill 64"), which targets private and public sector entities (as well as political parties) and, once adopted, will "result in significant changes to various laws in order to modernize the regulatory framework for the protection of personal data in Quebec".[1007] According to former Privacy Commissioner of Canada Jennifer Stoddart, with Bill 64, Quebec "takes the lead on privacy legislation in Canada".[1008] Bill 64 goes to committee at Quebec's National Assembly in fall 2020 and is expected to be adopted, with or without revisions, in spring 2021.[1009] If Bill 64 is passed, "both private and public sector organizations in Quebec would be subject to increased data protection obligations, in many ways similar to those imposed by the European Union's General Data Protection Regulations (GDPR)"[1010], including: "the right of erasure of information (often referred to as the right to be forgotten); the right of data portability (which allows customers to transfer personal information easily among organizations); and the right to receive notice if you are going to be subjected to surveillance"[1011]. Further, the Quebec Privacy Commissioner's enforcement powers would be strengthened (e.g., power to impose large monetary penalties on violators).

461. **Ontario privacy consultation.** On August 13, 2020, the Ontario government launched a public consultation on improving Ontario's privacy legislation, ending October 1, 2020[1012] ("Ontario privacy consultation"), specifically "to strengthen privacy protections of personal data", with an accompanying discussion paper ("Ontario Privacy Discussion Paper"). The reason for the consultation, according to Ontario Government and Consumer Services Minister Lisa Thompson, is that concerns about Ontario's privacy protections have "only been further highlighted during the COVID-19 outbreak" due to "Ontarians relying more on digital platforms to carry out day-to-day tasks" and "(w)ith the increased reliance on these platforms, there is a strong need to build public and consumer confidence and trust in the digital economy".[1013] The consultation solicits inputs on issues including enhanced consent provisions and new GDPR-like individual rights, and the Ontario Privacy Discussion Paper strongly suggests that Ontario plans to introduce private sector privacy legislation that is substantially similar to PIPEDA, in line with Alberta, BC, and Quebec.

462. **Supreme Court of Canada decision on privacy-impactful technology.** On July 10, 2020, the SCC ruled that the 2017 Genetic Non-Discrimination Act has a criminal law purpose and is within Parliament's jurisdiction under its constitutional criminal law powers. Teresa Scassa contends the decision "raises interesting issues about jurisdiction over privacy-impactful technologies" and could impact GoC's introduction of a bill to reform PIPEDA, which is expected "soon". In particular:

> *"(OPCC) has pressed the government to adopt a 'privacy as a human rights' approach in this reform process, but the government has seemed hesitant because of concerns that any emphasis on the human rights dimension of privacy might threaten the law's fragile constitutional footing under the trade and commerce power. The Supreme Court of Canada in the Reference re Genetic Non-Discrimination suggests that such an approach might not be as constitutionally risky as previously thought, although the risks are evidently there."*[1014]

463. **CJEU Shrems II decision.** On July 16, 2020, the Court of Justice of the European Union ("CJEU") released its "bombshell decision"[1015] in "Schrems II" invalidating the EU-US Data Protection Shield ("Privacy Shield") and "creating a new legal diligence burden on organizations" that rely on standard contractual clauses[1016]. Ann Cavoukian said the decision could have the knock-on effect of pushing GoC to update PIPEDA, while University of Victoria political science professor Colin Bennett said that due to the decision there must be "some serious, rather than cosmetic, reform to PIPEDA" and Quebec's proposed change to its privacy law, which comes close to GDPR, "ups the ante for the federal government".[1017]

PENDING BROADER PRIVACY LAW REFORM, IMPLEMENT PRIVACY-FIRST POLICY ON DCTT VIA RISK-MITIGATION STRATEGIES FOR CANADIAN GOVERNMENTS, REGULATORS & OWNER/OPERATORS OF DCTT (PUBLIC, PRIVATE & PUBLIC-PRIVATE)

464. **PIAC recommends that Privacy-First Policy on DCTT should, in interim, pending the outcomes of broader privacy legislation reform, be implemented via privacy risk-mitigation strategies deployed by Canadian governments, regulators (privacy commissioners and CRTC) and owner-operators of DCTT initiatives (public, private, and public-private).**

GOVERNMENT (FPT) PRIVACY RISK-MITIGATION STRATEGIES FOR DCTT

465. PIAC recommends that Canadian governments (FPT) should implement privacy risk-mitigation strategies that include the following.

466. **Emergency powers.** If warranted under COVID-19 pandemic circumstances (e.g., future "waves" of infection), GoC should set national, reasonable standards for personal data collection, use, and disclosure through DCTT, under its emergency powers and/or criminal law jurisdiction[1018], including[1019]:

- data is de-identified and aggregated, with protections (physical, technical, and administrative) against re-identification and disaggregation;
- data is encrypted, with security protections (legal and technical);
- data is information needed for established public health purposes only, except for clear, narrowly limited second purposes;
- data collection, use, and disclosure has strictly-enforced time limits, including specified end dates (with option to extend if needed) and, whether or not maintained in centralised database, destruction when crisis ends; and
- data is disclosed to PHAs only and, by corollary, not to other government institutions (e.g., law enforcement, border authorities, and other state agents) or businesses except in clear, narrowly limited circumstances.

467. Further, PT PHAs, if they believe their public health needs require it, should consider requesting use of their PT governments' emergency powers under emergency management legislation to access personal health information, for the purpose of digital contact tracing. PIAC would expect that governments would grant themselves these powers only in accordance with the May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance, that is, provided that these powers are used with caution (e.g., no fishing expeditions; used for purposes of contact tracing only; retained for as long as necessary), transparency, and accountability to PT privacy commissioners.

468. **Legislation to prevent governments and businesses from mandating use of CTAs (including *voluntary* official COVID Alert Canada)**. Governments (FPT) should implement legislation to prevent public and private entities from mandating use of or access to CTAs (in order to access goods, services, employment or places/spaces such as workplaces, housing, and parks), including the voluntary official COVID Alert Canada.

469. The OPCC privacy assessment of COVID Alert Canada notes: "it is possible that third parties may seek to compel use of the app or access to information in the app as a condition of service or employment" thereby "circumventing the voluntariness of the app and its single purpose"; some countries have laws against forcing people to use a CTA (e.g., Australia and Switzerland – see details above); however, in Canada "it is unclear whether the law would prohibit organizations from seeking information residing in the app, including whether the user has received an exposure notification, as a condition of service" and "it is another failing of our current laws that voluntariness and purpose limitation cannot be enforced clearly with measures such as those adopted in other countries".[1020] For this reason, OPCC recommends that *federal privacy legislation* should be amended to "*make enforceable against third parties* the voluntariness and purpose limitation principles" of COVID Alert Canada.[1021]

470. **PIAs.** Governments (FPT) should ensure that PIAs of official DCTT are conducted and submitted to relevant privacy commissioners *before deployment* and at *implementation* and *operation* stages, and consider court references for assessment of legality and constitutionality, where time permits.[1022] PIAC notes that Alberta Health's post-deployment submission of the ABTraceTogether PIA to the Alberta Commissioner is inconsistent with this recommendation, and acknowledges that pursuant to the "Interim Directive on Privacy Impact Assessment" the GoC PIA could be replaced with a "Privacy Compliance Evaluation".

471. **Audit powers.** Governments (FPT) should grant privacy commissioners the power to conduct independent audits of DCTT, where this power does not already exist, legislatively or through appropriate legal tools.[1023] Audits enable privacy commissioners to conduct ongoing monitoring and evaluation of these technologies for effectiveness at achieving their purpose(s), minimal intrusion, and security.[1024]

472. **Complaints.** Governments (FPT) should grant individuals the right to complain about DCTT to privacy commissioners, and a related right of action enforceable by courts, where this right does not already exist.[1025] According to the Criminal Lawyers' Association ("CLA"), "due process mechanisms must exist to enable individuals to seek recourse with respect to breaches, or misuse through digital contact surveillance powers, or to correct inaccurate or biased information collected or stored under such powers".[1026]

473. **Consultation.** Governments (FPT) should consult, on a proactive and ongoing basis, with privacy commissioners regarding developing, adopting, and deploying DCTT that is "privacy-respecting and trust-worthy"[1027]. PIAC notes that GoC's approach to developing COVID Alert Canada is inconsistent with this recommendation. On May 29, 2020, Privacy Commissioner Therrien told the INDU Committee that he had not yet been consulted about *any potential* official CTAs. When Health Minister Hajdu was asked on June 1, 2020 whether GoC would commit to consulting with Commissioner Therrien, she did not answer definitively, and only said privacy is a priority.[1028] OPCC told The Hill Times that Health Canada only submitted documentation on COVID Alert Canada (specifically a "privacy analysis" not a formal PIA) to its office on June 19, the day *after* PM Trudeau's endorsement of the app.[1029] The week of June 22, 2020, the BC, Saskatchewan, New Brunswick, and Nova Scotia privacy commissioners told the The Hill Times that GoC had not yet reached out to their offices.[1030]

REGULATOR (FPT) PRIVACY RISK-MITIGATION STRATEGIES FOR DCTT

PRIVACY COMMISSIONER (FPT) RISK-MITIGATION STRATEGIES FOR DCTT

474. PIAC recommends that Canadian privacy commissioners (FPT) should implement DCTT privacy risk-mitigation strategies that include the following.

475. **Privacy complaints.** Privacy commissioners (FPT) should expeditiously investigate privacy complaints about DCTT (if any), promptly issue a report of findings and, if applicable, recommendations for compliance ("Privacy Commissioner Report on Privacy and DCTT"), and immediately publish the report on grounds this is in the public interest. PIAC acknowledges this Report would be non-binding. Any finding of a privacy violation(s) will only work if the violator(s) voluntarily abide by it and comply with the recommendations or privacy commissioners enforce the law. This is a significant challenge, given certain FPT privacy commissioners (e.g., OPCC) have no order-making or fine-imposing powers and can only apply for a court order (e.g., Federal Court order), which is a lengthy and inefficient process that would likely outlast the COVID-19 pandemic.

476. **PIAs and audits.** OPCC should assert its right to review federal government PIAs or Privacy Compliance Evaluations of DCTT. FPT privacy commissioners should expeditiously review PIAs or Privacy Compliance Evaluations of DCTT that are submitted by governments and businesses and exercise their power, where it exists, to conduct independent audits.

477. **Consultation with CRTC.** As noted in today's Application to the CRTC, it may assist the CRTC if the OPCC considers network access of any CTAs, and we urge OPCC to communicate with CRTC in an effort to convince CRTC to investigate the network aspects of any app that may violate privacy under PIPEDA, the *Privacy Act* or the *Telecommunications Act*.

478. **Consultation and guidelines for privacy and COVID-19 DCTT.** Privacy commissioners (FPT) should consult, on a proactive and ongoing basis, with Canadian and international privacy experts regarding *evolved and strengthened* guidelines for privacy and COVID-19 DCTT that reflect global best practice in democratic countries' privacy policy responses. For example, CLA generally endorsed the May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance but elaborated on its privacy principles.[1031] PIAC recommends that strengthened privacy guidance should include the following privacy principles for COVID-19 DCTT:

- **Should be "conspicuous" and "right there in our faces"[1032]** – as suggested by international human rights lawyer Adam Gordon – to ensure Canadians remember these measures exist rather than forget about them (as PM Trudeau suggested) when life hopefully starts to return to some version of normalcy, so they can in turn ensure the government reverses these surveillance measures when the COVID-19 pandemic is done and refrains from introducing new ones to deal with lesser crises. As Mr. Gordon explains: "In essence, if we want to protect ourselves in the long-run from government overreach, we need the measures they implement in the short term to be annoying. The squeaky wheel get the grease (…) So let's make sure that the policy we get squeaks really loudly."[1033]
- **Should embrace PbD**, especially for official DCTT. In particular, official CTAs should be designed in a way that PHAs are the only effective data controllers or at least, if there are multiple actors, notify and explain their respective roles and responsibilities to users (e.g., via a comprehensive data flow analysis).
- **Should enforce fundamental legal requirement for consent to DCTTs.** PIAC believes the fundamental requirement for individual "consent" to the collection, use, and disclosure of personal information pursuant to existing Canadian privacy law is suited to the reality of the COVID-19 pandemic. It should be up to Canadians to make an informed decision on whether the advantages of using DCTT, especially CTAs (which are inherently generalized surveillance tools) outweigh their disadvantages. This sentiment is shared by global experts, including Greg Nojeim, Senior Counsel and Director of the Freedom, Security and Technology Project at the Centre for Democracy & Technology in Washington DC, who recently stated that "(i)t should be up to users to decide whether the benefits outweigh the disadvantages of using contact tracing apps".[1034] By corollary, PIAC rejects arguments made by certain advocates for the interests of data holders that:
  - "approaches relying too much on users' consent to protect privacy cannot adequately address infectious diseases such as COVID-19"; and
  - "the contact tracing discussion" which "has been framed as a choice between two options: consent or anonymization" (i.e., CTAs "must either secure individual's explicit consent or strip the data they collect of any identifying personal information") should embrace a third option: increased "accountability" for "open, authorized public purpose access" to personal data. [1035]

  We agree with Michael Geist that the appropriate standard of consent is the "emerging battle at the heart of privacy law" and, in the broader privacy law reform context, we will continue to vigorously object to the position of businesses that "have adopted exceptionally aggressive interpretations of the standards of consent, implying agreement to use personal information with little regard for the real intention, expectation or knowledge of individual Canadians" (e.g., "weaker opt-out models" versus "higher standards of opt-in consent").[1036]

CRTC PRIVACY RISK-MITIGATION STRATEGIES FOR DCTT

479. **Consultation with OPCC.** If CRTC identifies network access of any CTAs, or network-level DCTT, we urge CRTC to communicate with OPCC in an effort to convince OPCC to investigate the network aspects of any CTA or network-level DCTT that may violate privacy under PIPEDA, the Privacy Act or the Telecom Act.

DCTT OWNER/OPERATORS (PUBLIC, PRIVATE & PUBLIC-PRIVATE) PRIVACY RISK-MITIGATION STRATEGIES

480. PIAC recommends that owners/operators of DCTT (public, private, and public-private) should implement privacy risk-mitigation strategies that include the following.

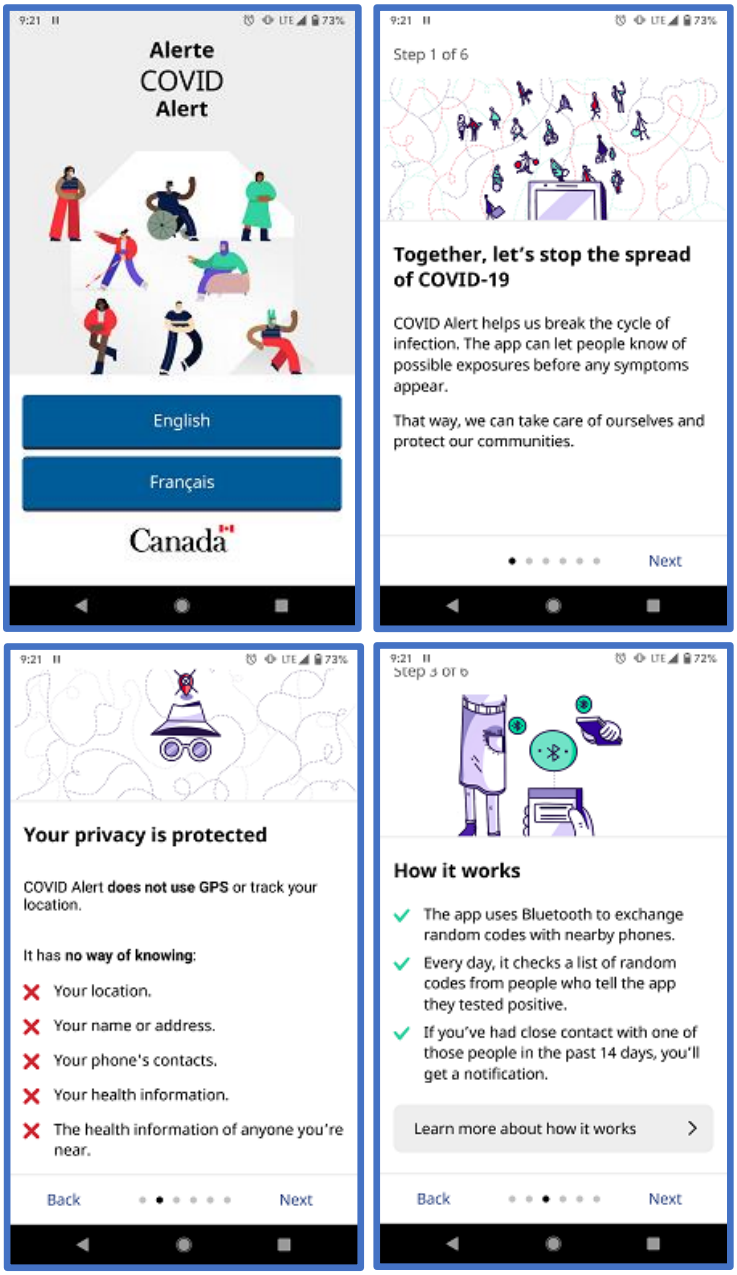
481. **PbD and PIAs.** Owners/operators of DCTT (official or unofficial) – especially those subject to Canadian privacy statutes – should *voluntarily*: employ PbD principles; and conduct PIAs and submit their PIA reports to the relevant privacy commissioner(s) *before deployment* and at *implementation and operation* stages and with adequate time to consider implementing any PIA recommendations. As OPCC emphasizes, "(d)one properly and before launching an initiative, PIAs can help ensure that legal (and policy) requirements are met and that privacy impacts are either addressed or minimized, before a problem occurs. In other parts of the world such as Europe, PIAs are becoming the legal standard".[1037]

CONCLUSION

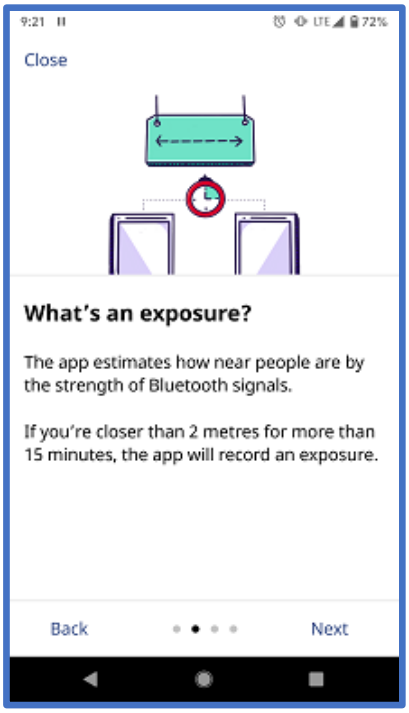
482. To summarize,

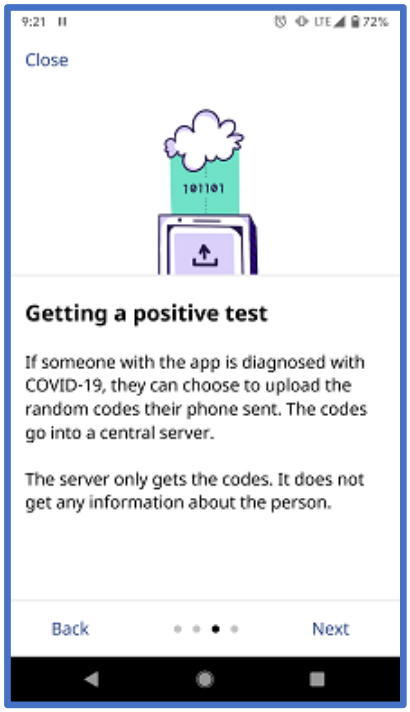
APPENDIX A: COVID ALERT CANADA SCREENSHOTS

COVID Alert Canada Introduction Screens

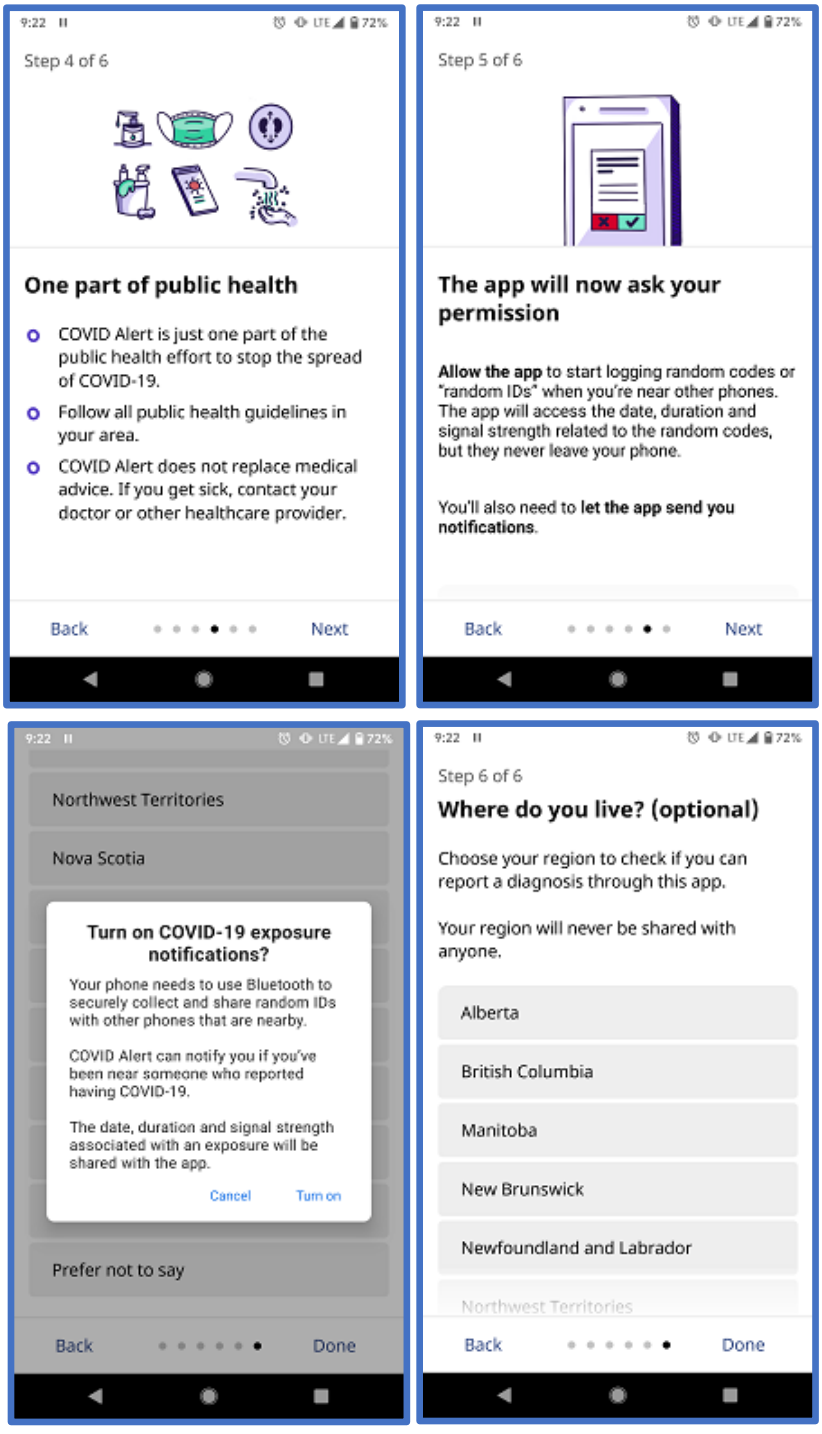


Learning About How COVID Alert Works

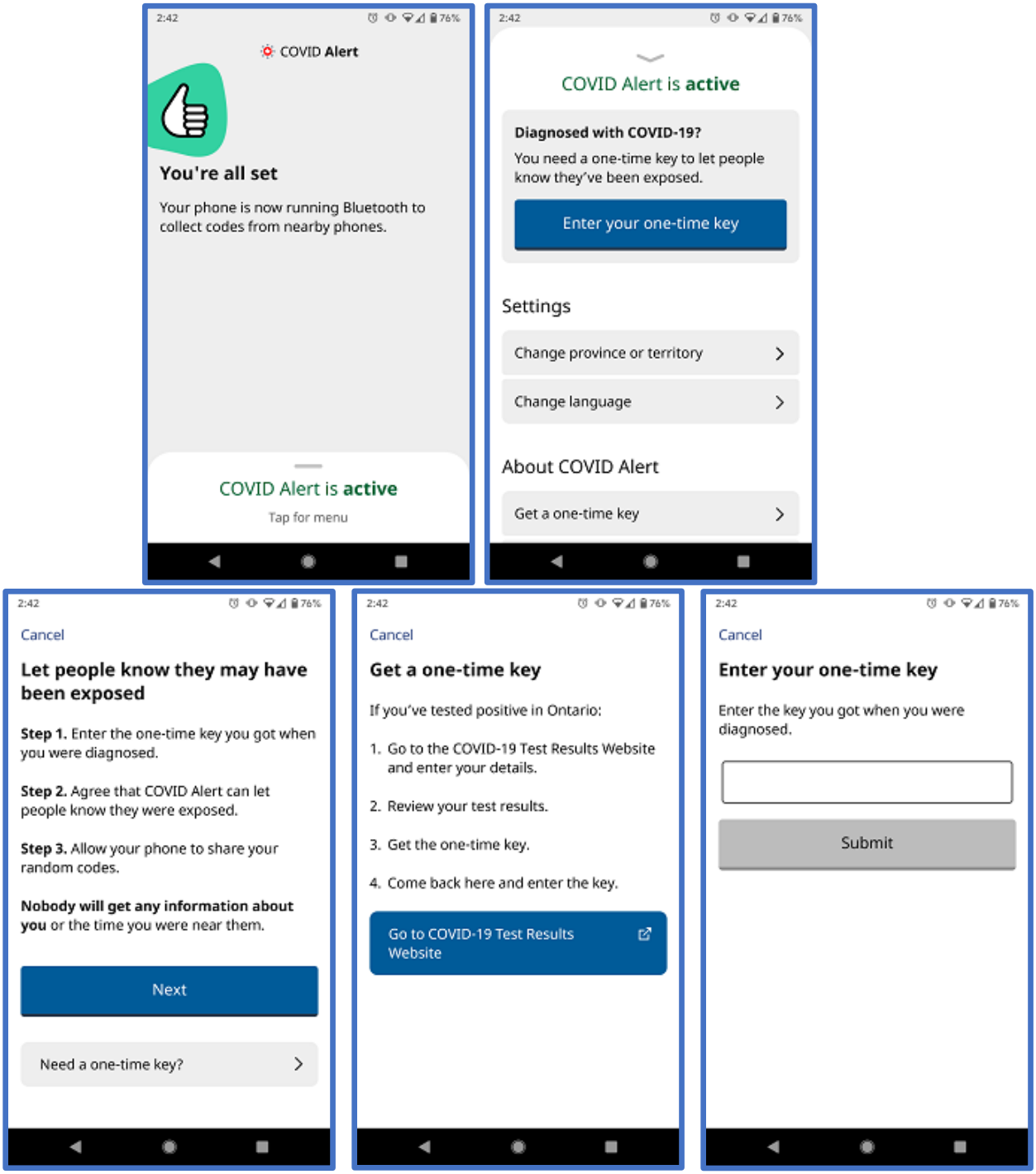




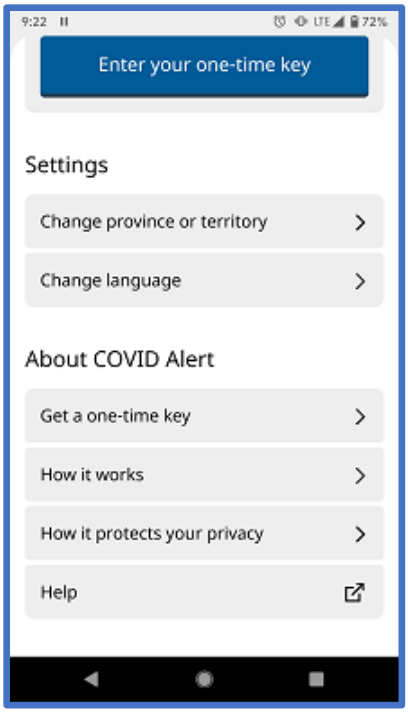
Turning On Exposure Notifications

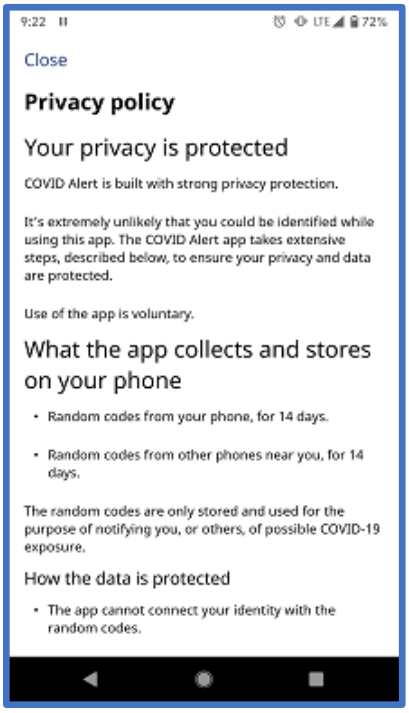


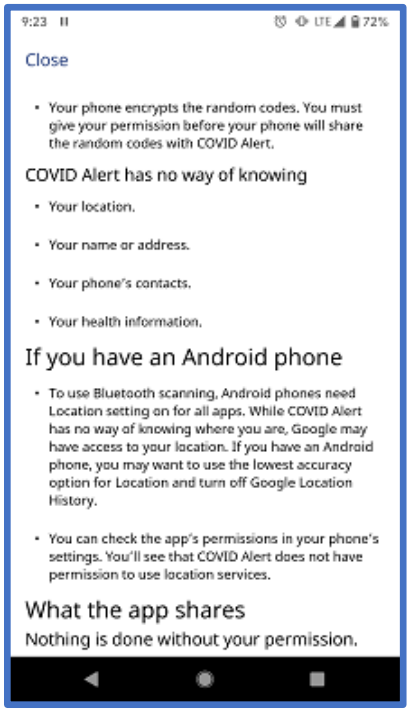
Entering The One-Time Key

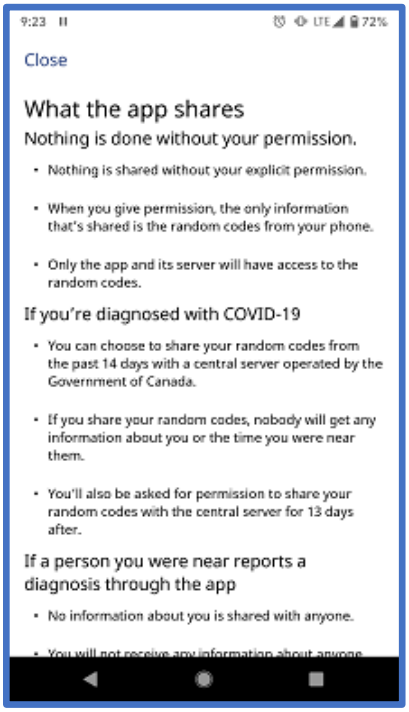


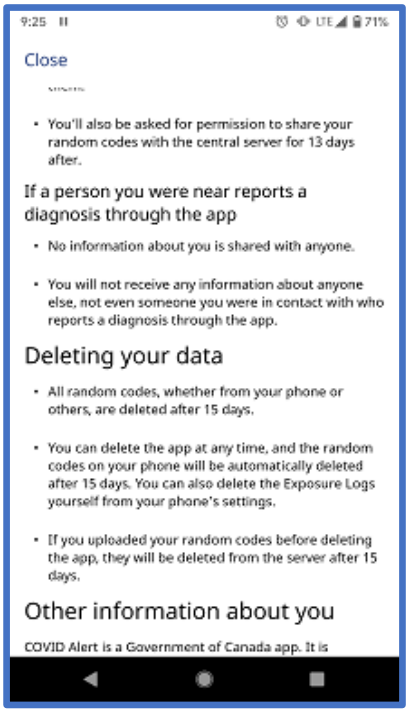
The Privacy Policy

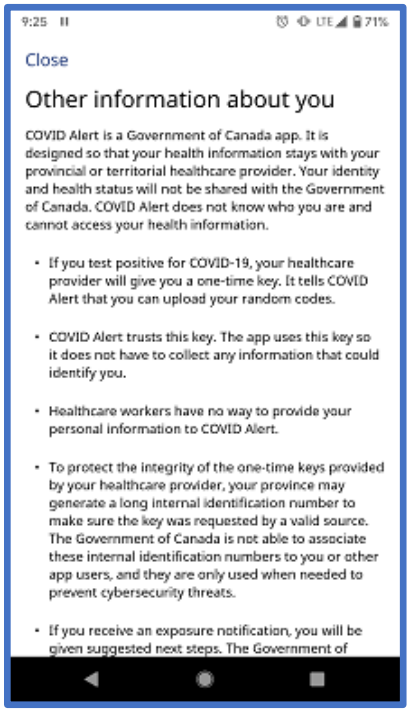




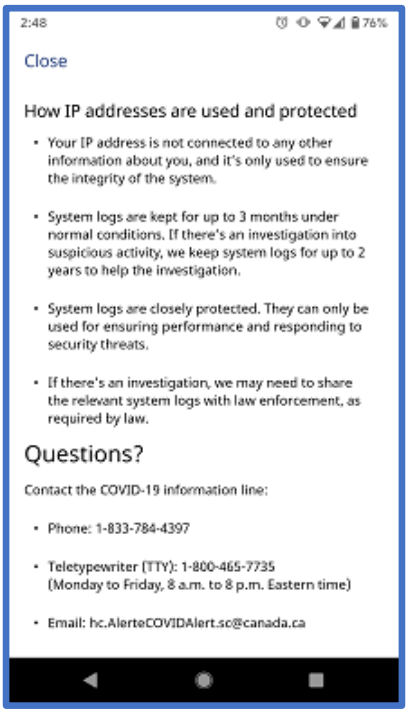




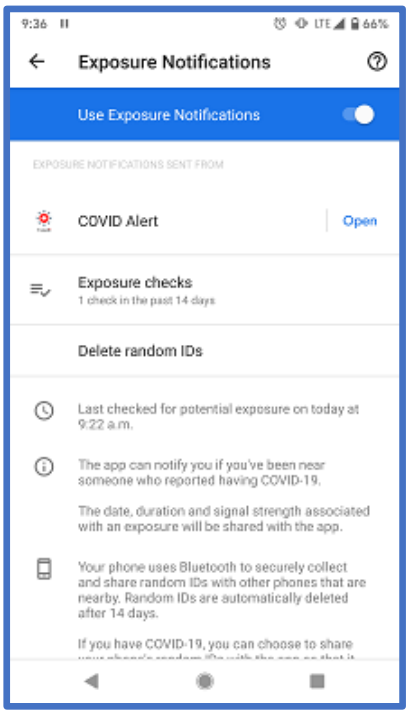


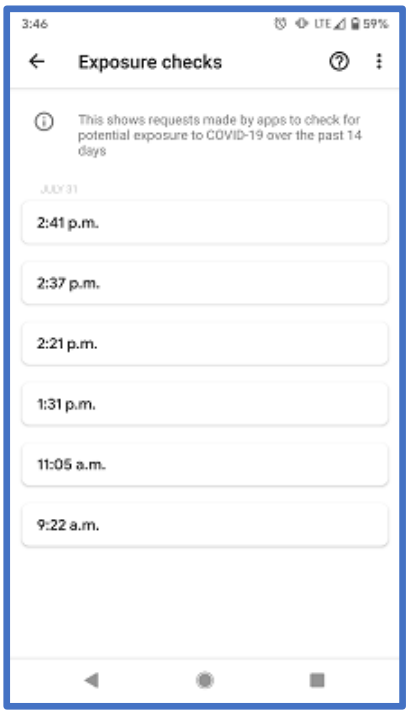


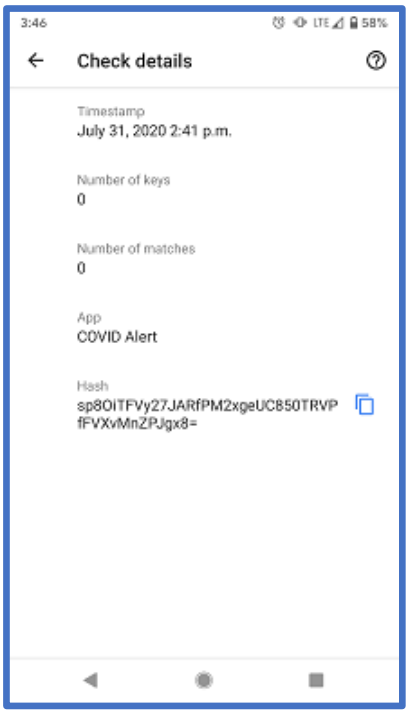
2:47
76%
Close
• If you receive an exposure notification, you will be given suggested next steps. The Government of Canada will not receive any health information about you if you take those next steps.
• COVID Alert does not connect with or collect any information from any other app on your phone.
Your IP address
As a security measure, the server will store your IP address in system logs when the app does any of the following actions:
• Download a list of positive codes.
• Enter a one-time key.
• Upload your random codes.
Without these security protections in place, spammers could flood the COVID Alert system and your phone with fake exposure notifications.
How IP addresses are used and protected
• Your IP address is not connected to any other information about you, and it's only used to ensure the integrity of the system.
• System logs are kept for up to 3 months under

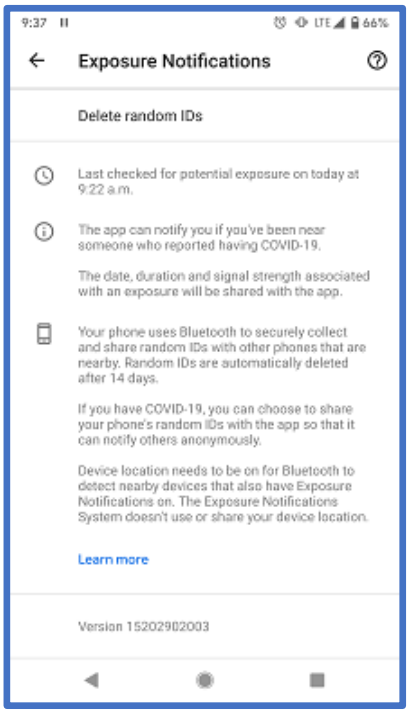

2:48
76%
Close
How IP addresses are used and protected
• Your IP address is not connected to any other information about you, and it's only used to ensure the integrity of the system.
• System logs are kept for up to 3 months under normal conditions. If there's an investigation into suspicious activity, we keep system logs for up to 2 years to help the investigation.
• System logs are closely protected. They can only be used for ensuring performance and responding to security threats.
• If there's an investigation, we may need to share the relevant system logs with law enforcement, as required by law.
Questions?
Contact the COVID-19 information line:
• Phone: 1-833-784-4397
• Teletypewriter (TTY): 1-800-465-7735
(Monday to Friday, 8 a.m. to 8 p.m. Eastern time)
• Email: hc.AlerteCOVIDAlert.sc@canada.ca

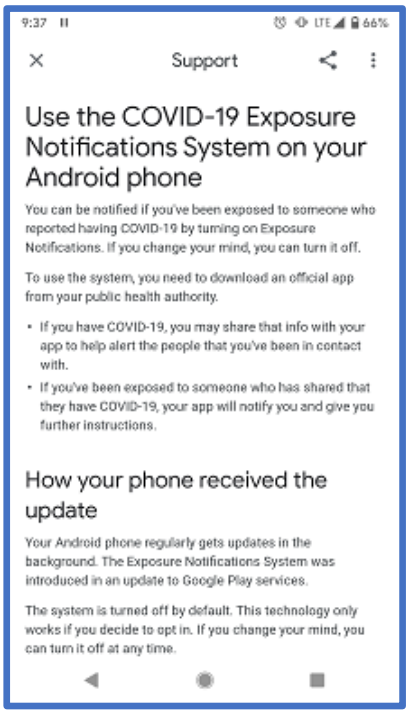
Exposure Notification Settings In Android Settings

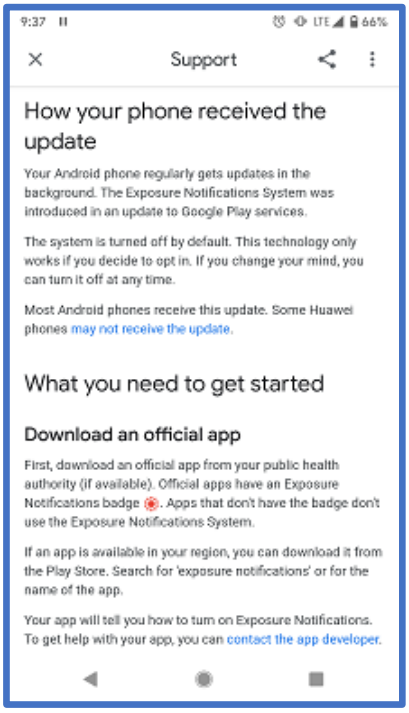


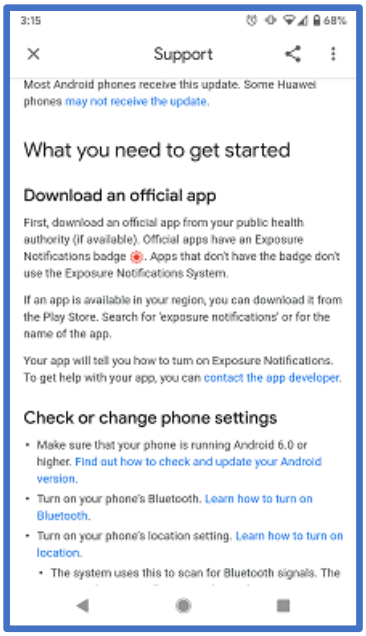


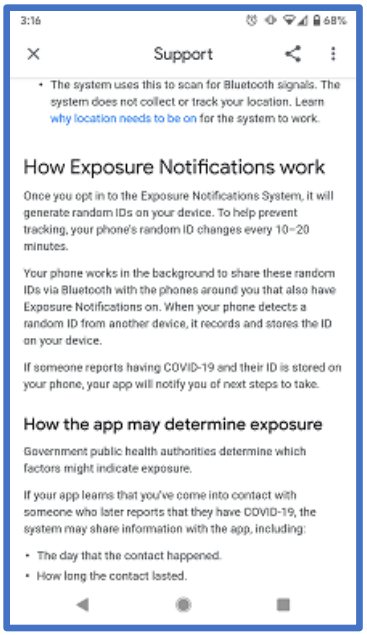


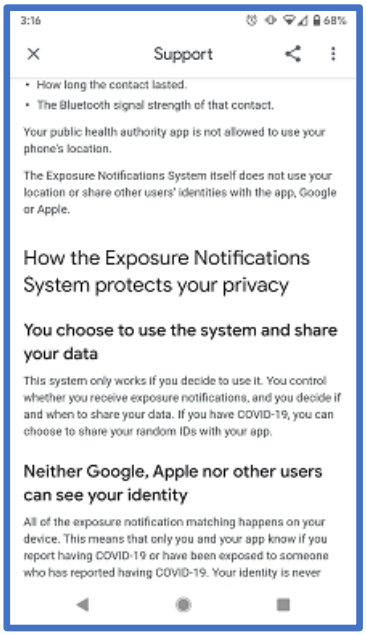


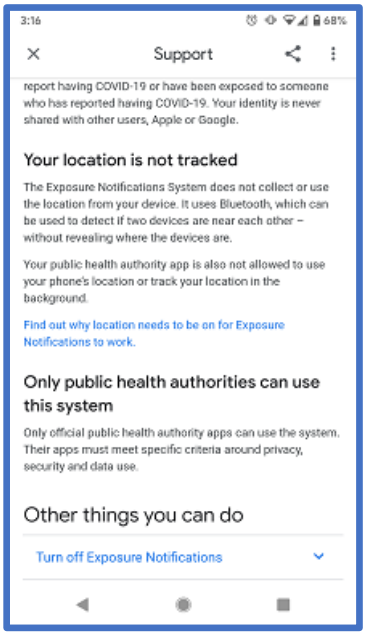


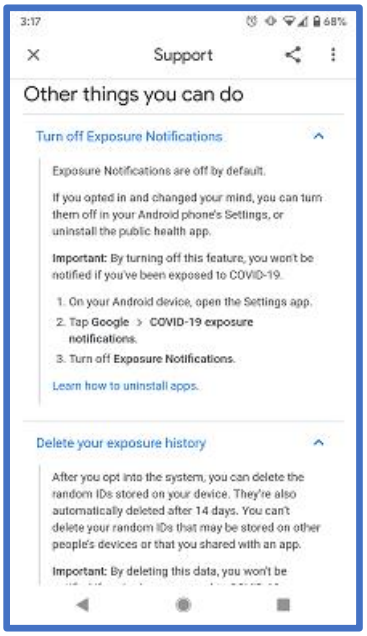


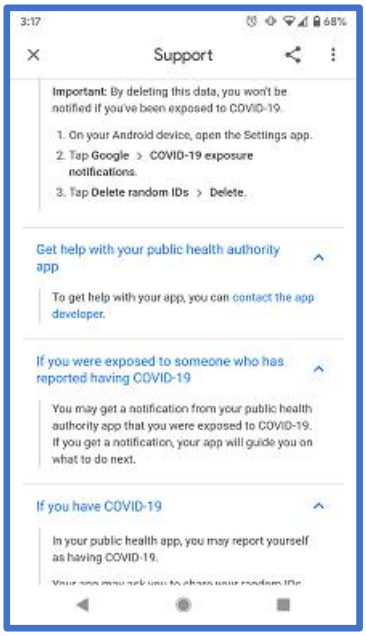

3:15
68%
Support
Most Android phones receive this update. Some Huawei phones may not receive the update.
What you need to get started
Download an official app
First, download an official app from your public health authority (if available). Official apps have an Exposure Notifications badge. Apps that don't have the badge don't use the Exposure Notifications System.
If an app is available in your region, you can download it from the Play Store. Search for 'exposure notifications' or for the name of the app.
Your app will tell you how to turn on Exposure Notifications. To get help with your app, you can contact the app developer.
Check or change phone settings
Make sure that your phone is running Android 6.0 or higher. Find out how to check and update your Android version.
Turn on your phone's Bluetooth. Learn how to turn on Bluetooth.
Turn on your phone's location setting. Learn how to turn on location.
The system uses this to scan for Bluetooth signals. The

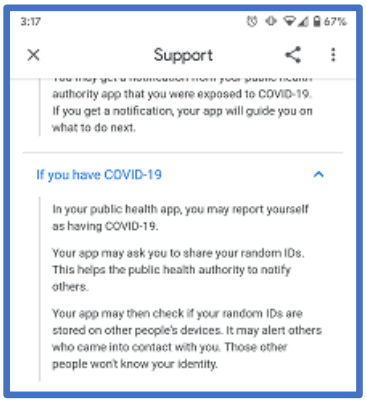

3:16
68%
Support
The system uses this to scan for Bluetooth signals. The system does not collect or track your location. Learn why location needs to be on for the system to work.
How Exposure Notifications work
Once you opt in to the Exposure Notifications System, it will generate random IDs on your device. To help prevent tracking, your phone's random ID changes every 10–20 minutes.
Your phone works in the background to share these random IDs via Bluetooth with the phones around you that also have Exposure Notifications on. When your phone detects a random ID from another device, it records and stores the ID on your device.
If someone reports having COVID-19 and their ID is stored on your phone, your app will notify you of next steps to take.
How the app may determine exposure
Government public health authorities determine which factors might indicate exposure.
If your app learns that you've come into contact with someone who later reports that they have COVID-19, the system may share information with the app, including:
The day that the contact happened.
How long the contact lasted.


3:16
68%
Support
How long the contact lasted.
The Bluetooth signal strength of that contact.
Your public health authority app is not allowed to use your phone's location.
The Exposure Notifications System itself does not use your location or share other users' identities with the app, Google or Apple.
How the Exposure Notifications System protects your privacy
You choose to use the system and share your data
This system only works if you decide to use it. You control whether you receive exposure notifications, and you decide if and when to share your data. If you have COVID-19, you can choose to share your random IDs with your app.
Neither Google, Apple nor other users can see your identity
All of the exposure notification matching happens on your device. This means that only you and your app know if you report having COVID-19 or have been exposed to someone who has reported having COVID-19. Your identity is never

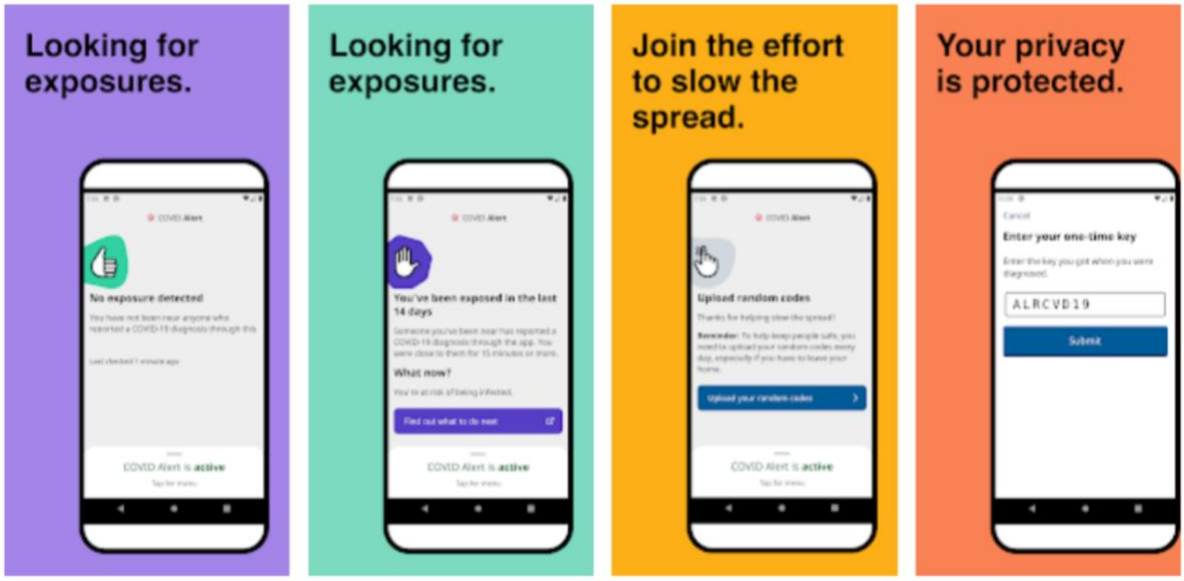

3:16
68%
Support
report having COVID-19 or have been exposed to someone who has reported having COVID-19. Your identity is never shared with other users, Apple or Google.
Your location is not tracked
The Exposure Notifications System does not collect or use the location from your device. It uses Bluetooth, which can be used to detect if two devices are near each other – without revealing where the devices are.
Your public health authority app is also not allowed to use your phone's location or track your location in the background.
Find out why location needs to be on for Exposure Notifications to work.
Only public health authorities can use this system
Only official public health authority apps can use the system. Their apps must meet specific criteria around privacy, security and data use.
Other things you can do
Turn off Exposure Notifications


3:17
68%
Support
Other things you can do
Turn off Exposure Notifications
Exposure Notifications are off by default.
If you opted in and changed your mind, you can turn them off in your Android phone's Settings, or uninstall the public health app.
Important: By turning off this feature, you won't be notified if you've been exposed to COVID-19.
1. On your Android device, open the Settings app.
2. Tap Google > COVID-19 exposure notifications.
3. Turn off Exposure Notifications.
Learn how to uninstall apps.
Delete your exposure history
After you opt into the system, you can delete the random IDs stored on your device. They're also automatically deleted after 14 days. You can't delete your random IDs that may be stored on other people's devices or that you shared with an app.
Important: By deleting this data, you won't be


3:17
68%
Support
Important: By deleting this data, you won't be notified if you've been exposed to COVID-19.
1. On your Android device, open the Settings app.
2. Tap Google > COVID-19 exposure notifications.
3. Tap Delete random IDs > Delete.
Get help with your public health authority app
To get help with your app, you can contact the app developer.
If you were exposed to someone who has reported having COVID-19
You may get a notification from your public health authority app that you were exposed to COVID-19. If you get a notification, your app will guide you on what to do next.
If you have COVID-19
In your public health app, you may report yourself as having COVID-19.


3:17
67%
Support
authority app that you were exposed to COVID-19. If you get a notification, your app will guide you on what to do next.
If you have COVID-19
In your public health app, you may report yourself as having COVID-19.
Your app may ask you to share your random IDs. This helps the public health authority to notify others.
Your app may then check if your random IDs are stored on other people's devices. It may alert others who came into contact with you. Those other people won't know your identity.

Positive Exposure Notification Screens (Publicly Available Images)



APPENDIX B: FEDERAL PRIVACY PRINCIPLES – PRIVACY ACT, PIPEDA & OPCC GUIDANCE

483. This Appendix provides an overview of key privacy principles and exceptions ("privacy principles") specific to federal privacy statutes, both public sector (Privacy Act) and private sector (PIPEDA), including pertinent OPCC and joint OPCC-PT privacy commissioner guidance *that relates to DCTT, particularly CTAs, both general and specific to COVID-19*. The reason is that one, some, or all of these could be implicated by present and/or future DCTT, both network- and application-level. This discussion begins with a summary of the acts' application, in terms of covered entities and personal information.

484. **Application (overall).** As noted, the Privacy Act regulates government institutions and PIPEDA regulates businesses, specifically:

Privacy Act: Covered Entities and Data

- The Privacy Act applies to only the approximately 250 federal government departments, agencies, and Crown corporations set out in the Act's "Schedule of Institutions", which include Health Canada[1038] ("covered entities"). The Act applies to *recorded* personal information, including federal employee information, that the federal government collects, uses, and discloses[1039] ("covered data").

PIPEDA: Covered Entities and Data

- According to the Department of Justice, as of June 5, 2020, PIPEDA "now generally applies to all private-sector organizations that collect, use or disclose personal information in the course of commercial activities in Canada"[1040] ("covered entities"). This includes federally regulated businesses, such as TSPs. PIPEDA does not apply to businesses (other than federally-regulated businesses) operating *within* PTs that have private sector privacy legislation deemed "substantially similar" to PIPEDA (i.e., Alberta[1041], BC[1042], and Québec[1043]), or to private health information custodians operating *within* PTs that have health privacy legislation deemed "substantially similar" to PIPEDA (i.e., Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia).[1044] PIPEDA applies to personal information and, for federally regulated businesses only, this includes employee information[1045] ("covered data").

485. Before identifying the key privacy principles under the acts and OPPC guidance, it is important to reiterate the May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance statement that: "Normal privacy laws apply unless emergency legislation provides otherwise." To date, no government – federal or PT – has invoked emergency management legislative powers to by-pass or use alternate authority *for contact tracing*. Any future emergency legislation that is constitutional and properly enacted could affect the below analysis.

PRIVACY PRINCIPLES UNDER PRIVACY ACT

486. **Quasi-constitutional status.** According to OPCC:

> *"The Supreme Court of Canada has stated that the Privacy Act has 'quasi-constitutional status', and that the values and rights set out in the Act are closely linked to those set out in the Constitution as being necessary to a free and democratic society. In particular it states that:*
>
> - *The government can only collect personal information that relates directly to one of its operating programs or activities;*
> - *Wherever possible, the information should be collected directly from the person it is about and the individual should be informed about the purpose of the collection;*
> - *The government should take all reasonable steps to ensure that the information it collects is accurate, up-to-date and complete;*
> - *The government may only use the personal information for the purposes that it collected it, or for a use consistent with that purpose (unless the individual consents to other uses), and*

- *Personal information may be disclosed by a government institution without an individual's consent where permitted under the Act. For example, it can be disclosed for the purpose of complying with warrants or court orders; where the disclosure is authorized in federal legislation; where disclosure would clearly benefit the individual, or where the public interest in disclosure outweighs the invasion of privacy."*[1046]

487. **Statutory requirements and privacy principles.** The Privacy Act does not contain privacy principles, a deficiency identified and criticized by stakeholders during the ongoing GoC legislative review.[1047] The Act does contain protections for recorded personal information[1048], however it primarily protects *individuals' access to their own* personal information[1049]. Covered entities have "fair information obligations" regarding collecting, maintaining, using, and disclosing personal information under their control, including[1050]:

- no personal information *shall* be collected unless it relates directly to an operating program or activity of the covered entity (section 4);
- wherever possible, personal information *should* be collected directly from the individual to whom it relates (section 5[1]), and s/he *should* be informed of the purpose for which it is being collected (section 5[2]). Personal information may be collected indirectly and without notice to the individual if direct collection and notice would result in the collection of inaccurate information or defeat the purpose or prejudice the use for which information is collected (subsection 5[3]);
- indexes indicating all "personal information banks (PIBs)" maintained by covered entities *must* be published (sections 10-11); and
- the "central privacy principle under the Act": that personal information under the control of a covered entity "shall not, without the consent of the individual to whom it relates, be used by the (entity) except for the purpose for which the information was obtained or compiled by the (entity) or for a use consistent with that purpose" (section 7). Put positively, covered entities must only use an individual's personal information for the purpose for which it was collected, or a use consistent with that purpose, *unless* the individual has provided consent.[1051]

488. Practically, the only point of the Privacy Act is that the department using the personal information has to describe the data collected and state which "databank" it is stored in, and convey that to Treasury Board, which then publishes a list of these databanks.

489. **Statutory exceptions/exemptions.** The Privacy Act "contain(s) a list of 13 uses and disclosures that might be permissible *without the consent* of the individual (e.g., national security, law enforcement, public interest)".[1052] Key exceptions are detailed below under the March 2020 OPCC COVID-19 Privacy Guidance.

PRIVACY PRINCIPLES UNDER PIPEDA

490. **Statutory requirements.** Covered entities may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (s. 5[3]) and must obtain *the knowledge and meaningful consent* of the individual for collecting, using, or disclosing their personal information (Principle 3 – see below). Consent is only valid if it is reasonable to expect the individual understands the nature, purpose, and consequences of the collection, use, or disclosure to which they are consenting (s. 6.1).

491. **Privacy principles.** PIPEDA sets out 10 "fair information principles" (aka "principles of fair information practices"), "which set up the basic privacy obligations under the law"[1053]:

> ***"1. Accountability** - Organizations should appoint someone to be responsible for privacy issues. They should make information about their privacy policies and procedures to available to customers.*

2. Identifying purposes *- Organization must identify the reasons for collecting your personal information before or at the time of collection.*

3. Consent *- Organizations should clearly inform you of the purposes for the collection, use or disclosure of personal information.*

4. Limiting collection *- Organizations should limit the amount and type of the information gathered to what is necessary.*

5. Limiting use, disclosure and retention *- In general, organizations should use or disclose your personal information only for the purpose for which it was collected, unless you consent. They should keep your personal information only as long as necessary.*

6. Accuracy *- Organizations should keep your personal information as accurate, complete and up to date as necessary.*

7. Safeguards *- Organizations need to protect your personal information against loss or theft by using appropriate security safeguards.*

8. Openness *- An organization's privacy policies and practices must be understandable and easily available.*

9. Individual access *- Generally speaking, you have a right to access the personal information that an organization holds about you.*

10. Recourse (Challenging compliance) *- Organizations must develop simple and easily accessible complaint procedures. When you contact an organization about a privacy concern, you should be informed about avenues of recourse."*[1054]

492. **Statutory exceptions.** Key PIPEDA exceptions to notice and consent (i.e., circumstances under which organizations may collect, use, or disclose personal information without notice or consent) are detailed below under March 2020 OPCC COVID-19 Privacy Guidance.

PRIVACY PRINCIPLES UNDER OPCC GUIDANCE (PRIVACY ACT & PIPEDA)

GENERAL GUIDANCE (KEY ONLY)

OPCC GUIDANCE ON MOBILE APPS

493. To help covered entities under the Privacy Act and PIPEDA through the PIA process, OPCC has issued guidance addressing various privacy issues, including biometrics, cloud computing, surveillance (overt and covert), and an October 2012 joint guidance with the Alberta and BC privacy commissioners on "mobile apps"[1055] that is targeted to app developers ("OPCC Guidance on Mobile Apps").[1056]

494. The OPCC Guidance on Mobile Apps states "there is an expectation and a legal requirement that app users are to be informed of what information is being collected, used and disclosed about them (…) and for their consent to be meaningful" and warns that app developers "can expect increased scrutiny of the privacy practices in your industry in the years ahead – both by regulators and the market itself". It also recommends that app developers should "(m)ake user privacy your competitive advantage" because "apps that take privacy seriously will be the ones that stand out from the crowd and gain user trust and loyalty".

495. Further, the guidance clarifies that PIPEDA could apply "(e)ven if you aren't generating revenue from an app" because "(c)ollecting, using and disclosing personal information to improve user experience, which indirectly contributes to the commercial success of your app, could still be considered a commercial activity".

496. Finally, the guidance sets out "key privacy considerations" for app developers ("either directly or through the company they work for") that include:

"You are accountable for your conduct and your code.

- *Your company, which may just be you, is responsible for all personal information collected, used and disclosed by your mobile app.*
- *Make sure to have controls in place, such as contracts or user agreements, to ensure that third parties accessing personal information through your app are respecting their privacy obligations.*
- *Map out where the information is going and identify potential privacy risks.*

Be open and transparent about your privacy practices.

- *Develop a privacy policy that informs users, in simple language, what your app is doing with their personal information.*
- *Post a privacy policy where users can easily find it, and where it is readily accessible to potential users who are considering downloading your app.*
- *Have a monitoring program in place to ensure that personal information is being handled in the way described in your privacy policy.*
- *When updating an app, inform users of any changes to the way their personal information is handled, and give them an easy way of refusing the update.*

Collect and keep only what your app needs to function, and secure it.

- *Limit data collection to what is needed to carry out legitimate purposes.*
- *Do not collect data because you think it may be useful in the future.*
- *Allow users to opt out of data collection outside of what they would reasonably expect is necessary for the functioning of the app.*
- *Have the appropriate safeguards in place to protect the personal information you are handling. Use encryption when storing and transmitting data.*
- *Give users the ability to delete the personal information your app has collected. If they delete the app, their data should be deleted automatically.*

Obtaining meaningful consent despite the small screen challenge.

- *Select the right strategy to convey privacy rules in a way that is meaningful on the small screen. This could include:*
  - *(L)ayering privacy information, placing important points up front and providing links to more detailed explanations.*
  - *A privacy dashboard that displays a user's privacy settings and provides a convenient means of changing them.*
  - *Visual cues such as graphics, colour and sound to draw user attention to what is happening with their personal information, the reasons for it, and choices available to the user.*

Timing of user notice and consent is critical.

- *Users should be told how their personal information is being handled at the time they download the app, when they first use the app, and throughout their app experience, to ensure that their consent remains meaningful and relevant.*
- *Be thoughtful and creative when deciding when to deliver privacy messages to most effectively capture users' attention and achieve the most impact at the right time, without causing notice fatigue. For example, if your app is about to actively tag photos with the user's location data, you could activate a symbol as a cue to the user, providing them with a choice to refuse."* [1057]

OPCC-ALBERTA & BC GUIDANCE ON MEANINGFUL CONSENT (INCL. LOCATION DATA)

497. OPCC and the Alberta and British Columbia Privacy Commissioner have jointly issued guidance on meaningful consent under PIPEDA[1058] ("OPCC Guidance on Meaningful Consent"), and it specifically addresses location data, which states:

> *"(I)f there is a use or disclosure a user would not reasonably expect to be occurring, such as certain sharing of information with a third party, the downloading of photos or contact lists, or the tracking of location, express consent would likely be required(.)"*

498. According to privacy law experts, a user granting a mobile app location permission (e.g., permission to access GPS on a user's mobile device) is not consenting to location tracking. For example, David Fraser, a privacy lawyer at McInnes Cooper in Halifax, says that under PIPEDA:

- "(c)ompanies need to be forthright in advance about what they're proposing to do with your information, and they have to get consent, and that consent has to be based on you understanding what is going on" and "(i)f they don't explain those purposes they would be offside the legislation";
- "(o)n an iOS device or Android device, an app is not able to find out your location unless you've given permission to the operating system to access your location information"; and
- "(t)here's a decision from the privacy commissioner of Canada that app permissions do not equal consent".[1059]

Bill Hearn, partner at law firm Fogler Rubinoff LLC in Toronto, offers the same interpretation of PIPEDA and observes that "industry has arguably flouted some of Canada's consent and privacy requirements because the consequences were not really meaningful and that (sic) there was not deterrence".[1060]

499. As of June 30, 2020, four Canadian privacy commissioners – OPCC, Alberta, BC, and Quebec – are formally investigating a Tim Hortons mobile app that, as discovered by an investigative journalist, conducts persistent location tracking and "knows where you sleep, work and vacation".[1061] The BC privacy commissioner also encouraged anyone with privacy concerns about the app to submit a privacy complaint.[1062] According to experts, a joint investigation by these privacy commissioners:

- is significant because B.C., Alberta, and Quebec are the only three PTs with their own private sector privacy legislation distinct from PIPEDA, indicating "they're looking to do an investigation that is relevant in every jurisdiction in Canada"; and
- highlights the flaws in Canadian privacy law, whereby investigations generally occur only in response to media reports and public attention (here, "really solid investigative journalism which, in turn, drew on some fairly sophisticated technical expertise to highlight the issue").[1063]

Additionally, the app is the subject of a class-action lawsuit in Quebec.[1064]

OPCC GUIDANCE ON DATA BREACHES

500. As noted above, while the term "data breach" is generally not expressly defined under Canadian privacy statutes, some refer to "breach of security safeguards" (e.g., PIPEDA s. 10.1 [1][1065]) or a similar term, effectively defined as *loss of, unauthorized access to, or unauthorized disclosure of* personal data resulting from a breach of an organization's safeguards or failure to establish those safeguards.[1066] There is no data breach provision in the Privacy Act.

501. On November 1, 2018, PIPEDA-covered entities became subject to new mandatory breach reporting regulations[1067], pursuant to which they must: report to OPCC "any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals" (commonly known as the "RROSH" test); "notify affected individuals about those breaches"; and "keep records of *all* data breaches within the organization".[1068] Further, OPCC has issued guidance on data breaches.[1069]

502. PIAC has on many prior occasions written about the insufficient federal solution for data breaches and recommended the Alberta approach (i.e., mandatory reporting of *all* data breaches to the privacy commissioner, who then decides whether the company must report to consumers/victims).

COVID-19 GUIDANCE

MAY 2020 JOINT OPCC-PT PRIVACY COMMISSIONER GUIDANCE TO FPT GOVERNMENTS ON DCTT

503. **Purpose.** The May 2020 Joint OPCC-PT Privacy Commissioner Guidance addresses the "extraordinary" measure of COVID-19 *DCTT*, including *CTAs*, which raise "important privacy risks" but "if done properly" can achieve both privacy and public health goals.[1070] The use of location data is specifically identified as a privacy concern.[1071]

504. **Application.** The May 2020 Guidance is intended to guide *FPT governments* in developing and implementing DCTT, however legal experts stress that "(t)echnology companies are well advised to keep (it) in mind when developing applications or other information tracing technologies for public sector institutions"[1072] (see details below).

505. **Privacy Principles.** The May 2020 Guidance outlines nine (9) privacy principles, including[1073]:

- Legal authority: Measures must have clear legal basis (i.e., governments must have legal authority to collect, use, and disclose personal information as part of its proposed program, activity, or initiative) and consent must be meaningful.
- Necessity and Proportionality: Measures must be science/evidence-based, necessary for a specific purpose (i.e., public health purpose – see next bullet), tailored to that purpose, likely to be effective to achieve that purpose, and the least intrusive option for that purpose
- Purpose Limitation: Personal information must be used for its intended *public health* purpose, and for no other purpose.
- Consent and trust: Apps must be voluntary, and separate consent must be obtained for each specific public health purpose.
- De-Identification: De-identified or aggregated data should be used whenever possible, unless it will not achieve the defined purpose, and consideration should be given to risk of re-identification (especially for location data).
- Time-Limitation: Measures should be time-limited (when crisis ends, any personal information collected should be destroyed and app decommissioned).
- Transparency: Governments should be clear about the basis and the terms applicable to measures (e.g., fully inform Canadians about what information will be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained, when it will be destroyed, and any associated risks, such as fraud or malware).
- Accountability: Governments should develop and make public an ongoing monitoring/evaluation plan of app effectiveness and commit to publicly posting evaluation report within specific timeframe and if app is not demonstrably effective, decommission it and destroy all personal data.
- Safeguards: Appropriate legal and technical security safeguards, including strong contracts between government institutions and app developers, must be put in place to prevent unauthorized access to data and ensure use of data is limited to the identified public health purpose(s). Data should not be accessible or compellable by service providers or other organizations.

506. **Proactive steps by technology companies.** Legal experts, consistent with the above-noted warning to technology companies, advises them to take certain "proactive steps" to "help to minimize the privacy

issues that may be raised by the applicable privacy commissioner when the client's PIA is formally reviewed"[1074]:

- Design DCTT (including CTAs) to comply with the foregoing privacy principles, applicable laws, and other best practices for personal information processing activities.
- Adopt a "privacy by design" framework.
- Ensure the technologies are "prepared in a manner that will allow a public sector institution to conduct a fulsome privacy impact assessment (PIA) with minimal disruption", noting:

  "At the federal level, a PIA is required where: (1) personal information is used as part of a decision-making process that directly affects an individual; and (2) the program or activity will have an impact on privacy. It is almost a certainty that a PIA will be required where a federal or provincial institution wishes to engage in contact tracing measures. In fact, a privacy impact assessment is currently underway by the Alberta Privacy Commissioner in connection with the implementation of contact tracing through smartphone technology through ABTraceTogether application."

507. **Relationship to April 2020 OPCC Guidance and international guidelines.** According to legal experts, the privacy principles in the May 2020 Joint OPCC-PT Privacy Commissioner Guidance: either "build on" (Miller Thomson) or are "the same as" (Bennett Jones LLP) the principles set out in the April 2020 OPCC Guidance (see details below); and are consistent with international privacy guidelines, particularly EU guidelines. According to law firm Miller Thomson:

> *"The EDPB [European Data Protection Board] generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures. The general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19."[1075]*

508. **Relationship to OPCC May 2020 comments on PIAs during COVID-19.** In a May 4, 2020 interview with The Hill Times, Privacy Commissioner Therrien said that a formal PIA "before an initiative is launched is the normal directive and is desirable", however:

> *"in an emergency situation, the government may proceed with a privacy-sensitive initiative with a serious privacy assessment, but not necessarily a fulsome PIA with all its usual rigour. There is some accommodation on some of the rules, but there needs to be a serious privacy assessment before something is launched."[1076]*

This is consistent with the above-noted modified TBS Directive on PIAs.

APRIL 2020 OPCC GUIDANCE TO GOC

509. **Purpose.** The April 2020 OPCC Guidance is intended to help *federal government institutions* by guiding "the development of privacy impactful initiatives that seek to alleviate the effects of the pandemic". CTAs are not expressly referenced, however the guidelines emphasize that "personal health information, and information about individuals' travel, movements and *contacts or association (…)* are generally considered *sensitive*" (emphasis added).

510. **Application.** According to legal experts (e.g., Bereskin & Parr and Winston & Strawn LLP), while the April 2020 Guidance is targeted at federal government institutions, a "majority" of the privacy principles it sets out also apply to businesses that are covered entities under PIPEDA.[1077]

511. **Privacy Principles.** The April 2020 OPCC Guidance sets out nine "key privacy principles that should factor into any assessment of measures proposed to combat COVID-19 that have an impact on the privacy of Canadians"[1078]. For "guidance on other privacy principles that continue to apply", readers are directed to "Expectations: OPC's Guide to the Privacy Impact Assessment Process", including its "Questions for high-risk

programs: necessity, effectiveness, proportionality and minimal intrusiveness".[1079] The nine privacy principles are[1080]:

- Legal authority: "Organizations" (here, "federal government institutions" and "private-sector organizations") must have a clear legal basis for collecting, using, and disclosing personal information, which may include information found on "public" sources (e.g., social media). This means: for government institutions, the Privacy Act; for businesses, PIPEDA or substantially similar PT legislation; and "special provisions that may be adopted under emergency laws". In "scenarios involving public-private partnerships":

  "where the lawful authority relied upon for collection is consent provided by individuals to a private-sector partner, the public-sector organization should approach its own collection of that information by ensuring the private-sector framework is properly applied, including meaningfulness of consent."[1081]

- Necessity and proportionality: "Government institutions" must ensure measures are necessary (here, necessary for a specific, identified purpose, evidence-based, and "likely to be effective") and proportionate (here, evidence- or science-based and not overbroad).
- Purpose Limitation: Only use personal information for the purpose it was collected (here, purpose of protecting public health, specifically "to alleviate the public health effects of COVID-19") and not for any other purpose (government or commercial).
- De-identification and other safeguarding measures:
  - Use de-identified or aggregated data where possible and minimize risk of re-identification (which is "highly case-specific – dependent on what data is used, in what form, and with what other data it is combined, and with whom it will be shared"), noting "unique challenges" of location data (i.e., is hard to fully de-identify and fully anonymize and data points themselves can lead to re-identification of an individual, especially home location, routine activities, and associations). Bereskin & Parr stresses that "(g)enerally speaking, information that is truly de-identified is not considered personal information and is therefore not subject to privacy legislation".[1082]
  - Protect personal information, especially sensitive, using administrative, technical, and physical means.
- Vulnerable populations: Consider disproportionate impacts of certain personal information on vulnerable populations and, if using AI, reduce inherent bias.
- Openness and transparency: Inform individuals of the purpose of collecting their personal information and provide clear, detailed, and ongoing information about new and emerging measures.
- Open data: Make data publicly available ("public datasets"), within reason, using de-identified data, and before releasing them assess benefits/risks of doing so, considering the context, particular risks (e.g., health and location data), and vulnerable populations.
- Oversight and accountability: Provide specific provision for oversight and accountability in new COVID-19 "laws and measures".
- Time limitation: Do not indefinitely retain *personal information*, including collected in an emergency, which should be destroyed when crisis ends (except for narrow purposes such as research or ensuring accountability for crisis decisions, especially about individuals). *Privacy-invasive measures* should be time-limited ("conservative, with the option to extend") and end when crisis is over.

512. **Relationship to May 2020 OPCC-PT Guidance and PIPEDA**. According to Bennett Jones LLP, these are "the same principles" as those set out in the May 2020 Joint OPCC-PT Privacy Commissioner Guidance and "(i)t is these same principles that form the backbone of the federal privacy legislation and provincial privacy legislation".[1083] However, according to Privacy Commissioner Therrien:

"There are several principles that we've put forward (in the April 2020 OPCC Guidance) that aren't provided for in the act, for example to use applications solely for public health tracing purposes. So

there's nothing in the present law that prevents a company to offer a tracing application that would allow that company to use the collected information for commercial purposes. There is just the requirement to obtain consent based on an ambiguous privacy policy".[1084]

513. **Relationship to March 2020 OPCC Guidance.** The April 2020 OPCC Guidance "accompanies" (OPCC)[1085], "compliments"[1086] (Bereskin & Parr), and "builds on" or "supplements" (Winston & Strawn LLP) the March 2020 OPCC Guidance (see details below).

MARCH 2020 OPCC GUIDANCE TO GOC & BUSINESSES

514. **Purpose and application.** The March 2020 OPCC Guidance, which clarifies that "privacy laws still apply, but they are not a barrier to appropriate information sharing" during the COVID-19 pandemic, is intended to help *federal government institutions and businesses* that are subject to federal privacy laws "understand their privacy-related obligations during the COVID-19 outbreak"[1087], pursuant to statutory requirements and relevant statutory exemptions (under the Privacy Act, PIPEDA, and emergency legislation).

515. **Exceptions to PIPEDA's notice and consent requirements.** The March 2020 Guidance highlights that PIPEDA provides specific exemptions to its *notice and consent* requirements that may be relevant during a health crisis such as COVID-19, including[1088]:

- *Collection* is clearly in the interests of the individual and consent cannot be obtained in a timely way (paragraph 7[1][a]) (e.g., individual is critically ill or in a particularly dangerous situation and needs help).
- *Collection and use* is for the purpose of making a disclosure required by law (paragraphs 7[1][e], 7[2][d] and 7[3][i]) (e.g., a PHA has legislative authority to require the disclosure).
- *Disclosure* is requested by a government institution under lawful authority to obtain the information and the disclosure is for the purpose of enforcing or administering any law of Canada or a province (subparagraphs 7[3][c.1][ii]-[iii]) (e.g., a PHA has legislative authority to require the disclosure).
- *Disclosure* is made on the organization's initiative to a government institution, which has reasonable grounds to believe the information relates to a breach of Canadian, PT, or foreign laws that has been, is being, or is about to be committed(paragraph 7[3][d][i]) (e.g., there is good-faith belief an individual is violating a valid quarantine order).
- *Use or disclosure* is for the purpose of acting in respect of an emergency that threatens an individual's life, health or security (paragraphs 7[2][b] and 7[3][e]) (e.g., individual requires urgent medical attention and is unable to communicate directly with medical professionals).

516. **Exceptions to Privacy Act's consent requirements.** The March 2020 Guidance highlights that the Privacy Act provides specific exemptions to its *consent* requirements that may be relevant during a health crisis such as COVID-19, including[1089]:

- *Disclosure* for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose [paragraph 8[2][a]), including if employers want to use their employee's phone number to provide updates about a pandemic.
- *Disclosure* where authorized by any other Act of Parliament or any regulation made thereunder that authorizes its disclosure (paragraph 8[2][b]), such as where a PHA has legislative authority to require the disclosure.
- *Disclosure* under an information sharing agreement between covered entities and PT governments, some First Nations councils, foreign governments, and international government organizations, for the purpose of enforcing any law or carrying out a lawful investigation (paragraph 8[2][f]) (e.g., GoC is represented in a multi-lateral information sharing agreement as part of the Pan-Canadian Public Health Network).

- *Disclosure* where, in the opinion of the head of the covered entity, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or where the disclosure would clearly benefit the individual to whom the information relates (paragraph 8[2][m]):

  "An example of this would be if the Deputy Minister of an institution deemed that a disclosure to another institution where an infected individual recently visited and may have spread the virus satisfied the balancing test. Although the Privacy Act specifies that the federal institution needs to notify the Privacy Commissioner in advance of a public interest disclosure, it also recognizes that in certain matters, time is of the essence. Where it is not reasonably practicable for the head of the government institution to inform the Commissioner in writing prior to the disclosure, notification to the Commissioner must be made as soon as possible after the fact (subsection 8[5]). If an institution suspects that the COVID-19 virus was spread or contracted in the workplace, it is recommended that the relevant public health authority be contacted to conduct any necessary contact tracing."

517. **Further expansion of powers to collect, use, and disclose personal information.** The March 2020 Guidance notes that where federal and PT governments formally declare public emergencies - which had been done in all PTs as of April 9, 2020[1090] - the powers to collect, use, and disclose personal information may be *further expanded.* However, the Guidance stresses that "normal" (i.e., existing) privacy laws apply unless emergency legislation states otherwise.[1091]

APPENDIX C: BIBLIOGRAPHY

GOVERNMENT – CANADA (FEDERAL & PROVINCIAL/TERRITORIAL ["FPT"])

GOVERNMENT OF CANADA ("GOC")

"Accessibility statement for COVID Alert", Government of Canada, July 31, 2020, online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/accessibility-statement.html (accessed August 2, 2020) ("Accessibility statement for COVID Alert").

"Canada extends mandatory requirements under the Quarantine Act for anyone entering Canada", Public Health Agency of Canada, June 30, 2020, online: https://www.canada.ca/en/public-health/news/2020/06/canada-extends-mandatory-requirements-under-the-quarantine-act-for-anyone-entering-canada.html ("Canada extends mandatory requirements under the Quarantine Act for anyone entering Canada").

"Canada's Digital Charter: trust in a digital world", Government of Canada, Innovation, Science and Economic Development Canada ("ISED"), May 21, 2019, online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html ("Canada's Digital Charter: trust in a digital world" or "Digital Charter").

"Canada's federal privacy laws: background paper", Publication No. 2007-44-E, Library of Parliament (Miguel Bernal-Castillero, Economics, Resources and International Affairs Division), October 1, 2013, online: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/200744E ("Canada's federal privacy laws: background paper").

"Canada's health care system", Government of Canada, online: https://www.canada.ca/en/health-canada/services/canada-health-care-system.html (accessed June 29, 2020) ("Canada's health care system").

"Canadian Network for Public Health Intelligence", Government of Canada, online: https://www.cnphi-rcrsp.ca/cnphi/index.jsp (accessed June 29, 2020) ("Canadian Network for Public Health Intelligence").

"Coronavirus disease (COVID-19): Travel restrictions, exemptions and advice", Government of Canada, online: https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/latest-travel-health-advice.html#a_arriveCAN (last modified August 12, 2020, accessed August 14, 2020) ("Coronavirus disease (COVID-19): Travel restrictions, exemptions and advice").

"COVID Alert: Exposure notification application privacy assessment", Health Canada, July 31, 2020 (last modified Aug 6, 2020), https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html ("Health Canada Privacy Assessment" or "COVID Alert: Exposure notification application privacy assessment").

"COVID-19 Exposure Notification App Advisory Council", Government of Canada, July 31, 2020, online: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/h_07687.html (accessed August 2, 2020) ("COVID-19 Exposure Notification App Advisory Council").

"COVID Alert Privacy Notice (Exposure Notification)", Health Canada, online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy.html (last updated August 6, 2020, accessed August 14, 2020) ("COVID Alert Privacy Notice [Exposure Notification]").

"Directive on identity management", Government of Canada, July 1, 2019, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577 (accessed June 18, 2020) ("GoC directive on identity management").

"Directive on personal information requests and correction of personal information", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32590 (last modified June 26, 2018; accessed June 18, 2020) ("GoC directive on personal information requests and correction of personal information").

"Directive on privacy impact assessment", Treasury Board of Canada Secretariat ("TBS"), April 1, 2010, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308 ("TBS Directive on privacy impact assessment").

"Directive on security management", Government of Canada, July 1, 2019, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611 (accessed June 18, 2020) ("GoC directive on security management").

"Directive on social insurance number", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342 (last modified May 16, 2008; accessed June 18, 2020) ("GoC directive on social insurance number").

"Download COVID Alert today", Health Canada, July 31, 2020, online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html (accessed August, 2, 2020) ("Download COVID Alert today").

"Fifth update report on developments in data protection law in Canada: Report to the European Commission June 2019", Government of Canada, ISED, online: https://www.ic.gc.ca/eic/site/113.nsf/eng/h_07666.html ("Fifth update report on developments in data protection law in Canada: Report to the European Commission June 2019").

"Frequently asked questions", Public Health Agency of Canada, online: https://www.canada.ca/en/public-health/corporate/mandate/about-agency/frequently-asked-questions.html (accessed July 28, 2020) ("Public Health Agency of Canada – FAQ").

"Guidance document: taking privacy into account before making contracting decisions", Treasury Board Secretariat, online: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-document-taking-privacy-into-account-before-making-contracting-decisions.html (accessed June 18, 2020) ("TBS guidance document: taking privacy into account before making contracting decisions").

"Guidance on preparing information sharing agreements involving personal information", Treasury Board Secretariat, July 2010, online: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html#a664Protectionof (accessed June 18, 2020) ("TBS guidance on preparing information sharing agreements involving personal information").

"Guidelines for privacy breaches", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154 (last modified May 20, 2014, accessed June 18, 2020) ("GoC guidelines for privacy breaches").

"Health Portfolio", Government of Canada, online: https://www.canada.ca/en/health-canada/corporate/health-portfolio.html (accessed June 12 and 29, 2020) ("Health Portfolio" or "GoC health portfolio").

"Interim directive on privacy impact assessment", Treasury Board Secretariat, March 13, 2020, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=html (last modified June 18, 2020; accessed July 31, 2020) ("Interim directive on privacy impact assessment").

"Interim directive on privacy practices", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309 (last modified June 18, 2020; accessed June 18, 2020) ("GoC interim directive on privacy practices").

"Interim policy on privacy protection", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510 (last modified June 18, 2020; accessed June 18, 2020) ("GoC interim policy on privacy protection").

"IT security risk management: a lifecycle approach (ITSG-33)", Canadian Centre for Cyber Security, online: https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33 (accessed June 18, 2020) ("Canadian Centre for Cyber Security IT security risk management").

"Minister of Canadian Heritage mandate letter", Office of the Prime Minister, December 13, 2020, online: https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-canadian-heritage-mandate-letter ("December 2019 Heritage Minister mandate letter").

"Minister of Innovation, Science and Industry mandate letter", Office of the Prime Minister, December 13, 2020, online: https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-innovation-science-and-industry-mandate-letter ("December 2019 ISI Minister mandate letter").

"Modernizing Canada's Privacy Act", Government of Canada, Department of Justice, online: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html (last modified June 6, 2020; accessed June 9 and August 17, 2020) ("Modernizing Canada's Privacy Act").

"Modernizing Canada's Privacy Act: what we heard report – summer and fall 2019", Government of Canada, Department of Justice, June 5, 2020, online: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/wwh-cqnae/index.html ("Modernizing Canada's Privacy Act: what we heard report – summer and fall 2019").

"MP Charlie Angus letter to ISI Minister Bains re: privacy issues arising from contact tracing apps", June 11, 2020, online: https://69490847-1bbc-4d85-bb17-dc869f025e9a.filesusr.com/ugd/3c9b44_df698b38bee249e88d4fcc2df696e314.pdf?utm_source=The+Logic+Master+List&utm_campaign=517c6e4fb4-Daily_Briefing_2020_June12_2&utm_medium=email&utm_term=0_325d5d3b52-517c6e4fb4-275653649 ("MP Charlie Angus letter to ISI Minister Bains re: privacy and contact tracing apps").

"MP Charlie Angus letter to Privacy Commissioner of Canada re: contact tracing apps", June 8, 2020, online: https://69490847-1bbc-4d85-bb17-dc869f025e9a.filesusr.com/ugd/3c9b44_f9618c058c0e47f18a38eb836f5fe808.pdf?utm_source=The+Logic+Master+List&utm_campaign=777c4566c3-Daily_Briefing_2020_June9_2&utm_medium=email&utm_term=0_325d5d3b52-777c4566c3-275653649 ("MP Charlie Angus letter to Privacy Commissioner of Canada re: contact tracing apps").

"News Release: Conservatives request Privacy Commissioner investigate federal contact tracing app and ArriveCAN app", July 29, 2020 ("News Release: Conservatives request Privacy Commissioner investigate federal contact tracing app and ArriveCAN app"). (note: includes link to letter dated July 29, 2020)

"Notice: Health Canada's approach to digital health technologies", Government of Canada, April 10, 2018, online: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html ("Notice: Health Canada's approach to digital health technologies").

"Policy on government security", Government of Canada, online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578 (last modified July 1, 2019; accessed June 18, 2020) ("GoC policy on government security").

"Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure", Prime Minister's Office ("PMO") News Release, June 18, 2020, online: https://pm.gc.ca/en/news/news-releases/2020/06/18/prime-minister-announces-new-mobile-app-help-notify-canadians-covid ("Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure").

"Privacy impact assessment", Statistics Canada, online: https://www.statcan.gc.ca/eng/about/pia/pia (accessed June 9, 2020) ("Statistics Canada, privacy impact assessment").

"Speech: Prime Minister's remarks on COVID-19 measures and the launch of the COVID Alert national application", Justin Trudeau, Prime Minister of Canada, July 31, 2020, online: pm.gc.ca/en/news/speeches/2020/07/31/prime-ministers-remarks-covid-19-measures-and-launch-covid-alert-national ("Speech: Prime Minister's remarks on COVID-19 measures and the launch of the COVID Alert national application").

"Strengthening privacy for the digital age: proposals to modernize the Personal Information Protection and Electronic Documents Act", Government of Canada, ISED, online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html ("Strengthening privacy for the digital age: proposals to modernize the Personal Information Protection and Electronic Documents Act" or "GoC proposals to modernize PIPEDA").

"Terms of Reference of the Advisory Council to federal, provincial and territorial governments on the national COVID-19 exposure notification app", ISED, online: www.ic.gc.ca/eic/site/icgc.nsf/eng/07688.html ("Terms of Reference of the Advisory Council to federal, provincial and territorial governments on the national COVID-19 exposure notification app").

"The governments of Canada and Quebec and the international community join forces to advance the responsible development of artificial intelligence", Government of Canada, ISED, June 15, 2020, online: https://www.canada.ca/en/innovation-science-economic-development/news/2020/06/the-governments-of-canada-and-quebec-and-the-international-community-join-forces-to-advance-the-responsible-development-of-artificial-intelligence.html ("The governments of Canada and Quebec and the international community join forces to advance the responsible development of artificial intelligence").

Tweet by Senator Deacon re: COVID Alert Canada launch, July 31, 2020 ("Tweet by Senator Deacon, July 31, 2020").

"Vulnerability disclosure process for the COVID Alert service", Canadian Digital Service ("CDS") & Office of the Chief Information Officer, July 31, 2020, online: https://github.com/cds-snc/covid-alert-documentation/blob/main/VulnerabilityDisclosurePolicy.md (accessed August 2, 2020) ("Vulnerability disclosure process for the COVID Alert service").

PROVINCIAL/TERRITORIAL ("PT") GOVERNMENTS

ALBERTA ("AB")

"ABTraceTogether FAQ", Alberta Government, online: https://www.alberta.ca/ab-trace-together-faq.aspx (accessed 29 May 2020) ("ABTraceTogether FAQ").

"Commissioner Comments on Alberta's Contract Tracing App", Alberta Office of the Information and Privacy Commissioner ("Alberta OIPC"), May 1, 2020, online: https://www.oipc.ab.ca/news-and-events/news-releases/2020/commissioner-comments-on-alberta%E2%80%99s-contact-tracing-app.aspx ("Commissioner Comments on Alberta's Contract Tracing App").

BRITISH COLUMBIA ("BC")

N/A

MANITOBA ("MB")

N/A

NEW BRUNSWICK ("NB")

N/A

NEWFOUNDLAND AND LABRADOR ("NL + LD")

N/A

NORTHWEST TERRITORIES ("NWT")

N/A

NOVA SCOTIA ("NS")

N/A

NUNAVUT ("NU")

N/A

ONTARIO ("ON")

"COVID-19 contact tracing initiative", Public Health Ontario, online: https://www.publichealthontario.ca/en/diseases-and-conditions/infectious-diseases/respiratory-diseases/novel-coronavirus/contact-tracing-initiative (accessed 20 May 2020) ("Public Health Ontario COVID-19 contact tracing initiative")

"COVID-19 test results website Terms of Use", Ontario Health, online: covid19results.ehealthontario.ca:4443/terms ("COVID-19 test results website Terms of Use").

"Declaration of PHIPA as substantially similar to PIPEDA", Ontario Ministry of Health and Long-Term Care, online: http://www.health.gov.on.ca/english/providers/project/priv_legislation/phipa_pipeda_qa.html (accessed August 14, 2020) ("Declaration of PHIPA as substantially similar to PIPEDA").

"Discussion paper: Ontario private sector privacy reform", Ontario Government, Ministry of Government and Consumer Services, August 13, 2020, online: https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45105 ("Discussion paper: Ontario private sector privacy reform").

"Emergency information: provincial status on COVID-19, update on July 31", Government of Ontario, online: https://www.ontario.ca/page/emergency-information ("Emergency information: provincial status on COVID-19, update on July 31").

"Ontario appoints Special Advisor to develop health data platform", Ontario government, June 4, 2020, online: https://news.ontario.ca/mohltc/en/2020/06/ontario-appoints-special-advisor-to-develop-health-data-platform.html?utm_source=ondemand&utm_medium=email&utm_campaign=p ("Ontario appoints Special Advisor to develop health data platform").

"Ontario enhancing COVID-19 case and contact management", Government of Ontario, News Release, June 18, 2020, online: https://news.ontario.ca/opo/en/2020/06/ontario-enhancing-covid-19-case-and-contact-management.html?utm_source=ondemand&utm_medium=email&utm_campaign=p ("Ontario Enhancing COVID-19 case and contact management").

"Ontario expanding data collection to help stop spread of COVID-19", Government of Ontario, News Release, June 15, 2020, online: https://news.ontario.ca/mohltc/en/2020/06/ontario-expanding-data-collection-to-help-stop-spread-of-covid-19.html?utm_source=ondemand&utm_medium=email&utm_campaign=p ("Ontario expanding data collection to help stop spread of COVID-19").

"Ontario extends declaration of Emergency to July 15", Government of Ontario, News Release, June 24, 2020, online: https://news.ontario.ca/opo/en/2020/06/ontario-extends-declaration-of-emergency-to-july-15.html ("Ontario extends declaration of Emergency to July 15").

"Ontario extends Emergency Orders to July 10", Government of Ontario, News Release, June 27, 2020, online: https://news.ontario.ca/opo/en/2020/06/ontario-extends-emergency-orders-to-july-10.html?utm_source=ondemand&utm_medium=email&utm_campaign=p ("Ontario extends Emergency Orders to July 10").

"Ontario extends Emergency Orders", Government of Ontario, July 16, 2020, online: https://news.ontario.ca/opo/en/2020/07/ontario-extends-emergency-orders-2.html ("Ontario extends Emergency Orders to July 29, 2020").

"Ontario opens up COVID-19 testing across the province", Ontario Government, May 29, 2020, online: https://news.ontario.ca/opo/en/2020/05/ontario-opens-up-covid-19-testing-across-the-province.html ("Ontario opens up COVID-19 testing across the province").

"News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19", Office of the Premier, July 31, 2020, online: news.ontario.ca/opo/en/2020/07/covid-alert-available-for-download-beginning-today.html ("News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19").

"News Release: Ontario implementing additional measures at bars and restaurants to help limit the spread of COVID-19: measures to further protect the health of Ontarians as the province continues to re-open under Stage 3", Ontario Ministry of Health, July 31, 2020 (**"**News Release: Ontario implementing additional measures at bars and restaurants to help limit the spread of COVID-19").

"News release: Ontario launches consultations to strengthen privacy protections of personal data", Ontario Ministry of Government and Consumer Services, August 13, 2020, online: https://news.ontario.ca/mgs/en/2020/08/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data.html?utm_source=ondemand&utm_medium=email&utm_campaign=p ("News release: Ontario launches consultations to strengthen privacy protections of personal data").

"News Release: Ontario legislature adjourns after significant sitting in response to COVID-19", Government of Ontario, July 22, 2020 ("News Release: Ontario legislature adjourns after significant sitting in response to COVID-19").

Orders and Notices Paper No. 174, Legislative Assembly of Ontario, July 13, 2020, online: https://www.ola.org/sites/default/files/node-files/house/document/pdf/2020/2020-07/174_July_13_2020_Orders_0.pdf ("Ontario extends declaration of emergency until July 24, 2020").

PRINCE EDWARD ISLAND ("PEI")

N/A

QUEBEC ("QC")

Bill for *An Act to Modernise Legislative Provisions as Regards the Protection of Personal Information*, introduced June 12, 2020, online: http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bll.DocumentGenerique_159567en&process=Default&token=ZyMoxNwUn8ikQ+TRKYwPCjWrKwg+vIv9rjij7p3xLGTZDmLVSmJLoqe/vG7/YWzz ("Quebec Bill for *An Act to Modernise Legislative*

Provisions as Regards the Protection of Personal Information, introduced 12 June 2020"). (note: Bill's progress can be tracked here: http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html)

SASKATCHEWAN ("SK")

N/A

YUKON ("YK")

N/A

REGULATORS

CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION ("CRTC")

Letter determination re: Application submitted by the Public Interest Advocacy Centre regarding pandemic contact-tracing by major Canadian telecommunications service providers, CRTC, Ottawa, August 17, 2020 ("CRTC decision letter on May 2020 PIAC Part 1 Application on Contact Tracing").

PIAC response to procedural requests to dismiss Part 1 Application Regarding Pandemic Contact-Tracing, 12 May 2020 ("PIAC response to procedural requests to dismiss May 2020 Part 1 Application").

PIAC Telecom Part I Application Regarding Pandemic Contact-Tracing at Application and Network Levels by Major Canadian TSPs, May 4, 2020 ("May 2020 PIAC Part 1 Application Regarding Pandemic Contact Tracing" or "May 2020 PIAC Part 1 Application on Contact Tracing").

PRIVACY COMMISSIONERS

OVERALL/JOINT

"Guidelines for obtaining meaningful consent", OPC, Alberta Privacy Commissioner, and British Columbia Privacy Commissioner, May 2018, online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ ("Joint OPCC and Alberta and BC Privacy Commissioner 2018 Guidance on Meaningful Consent").

"News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness", OPC and Ontario IPC, July 31, 2020, online https://www.ipc.on.ca/newsrelease/federal-and-ontario-privacy-commissioners-support-use-of-covid-alert-application-subject-to-ongoing-monitoring-of-its-privacy-protections-and-effectiveness/ ("News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness").

"Seizing opportunity: good privacy practices for developing mobile apps", joint OPC and Alberta and British Columbia Privacy Commissioner Guidance, October 2012, online: https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/ ("Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps").

"Supporting public health, building public trust: privacy principles for contact tracing and similar apps - joint statement by federal, provincial and territorial Privacy Commissioners", May 7, 2020, online: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/ ("May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance").

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA ("OPCC" OR "OPC")

"2019-20 Departmental Plan", OPC, online: https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2019-2020/dp_2019-20/ ("OPC 2019-20 Departmental Plan").

"A Data Privacy Day conversation with Canada's Privacy Commissioner", Privacy Commissioner of Canada (Daniel Therrien), Remarks at the University of Ottawa's Centre for Law, Technology and Society, January 28, 2020, online: https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200128/ ("A Data Privacy Day conversation with Canada's Privacy Commissioner").

"A framework for the Government of Canada to assess privacy-impactful initiatives in response to COVID-19", April 2020, online: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/ ("A framework for the Government of Canada to assess privacy-impactful initiatives in response to COVID-19" or "April 2020 OPCC COVID-19 Privacy Guidance").

"A full year of mandatory data breach reporting: what we've learned and what businesses need to know", OPC, October 31, 2019, online: https://www.priv.gc.ca/en/blog/20191031/ (accessed July 21, 2020) ("A full year of mandatory data breach reporting: what we've learned and what businesses need to know").

"A guide for individuals protecting your privacy", OPC, online: https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/ (accessed 21 May and 17 June 2020) ("OPC a guide for individuals protecting your privacy").

"Expectations: OPC's guide to the privacy impact assessment process", OPC, revised March 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/ ("Expectations: OPC's guide to the privacy impact assessment process" or "Expectations: OPC's guide to the privacy impact assessment process, March 2020").

"Federal Court applications under the Privacy Act", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/federal-court-applications-under-the-privacy-act/ (accessed June 18, 2020) ("Federal Court applications under the Privacy Act").

"Office of the Privacy Commissioner of Canada", OPC, online: https://www.priv.gc.ca/.

"OPC guide on personal information retention and disposal: principles and best practices", OPC, June 2014, online: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/ (accessed June 18, 2020) ("OPCC Guide on personal information retention and disposal").

"OPC privacy impact assessments", OPC, online: https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/opc-privacy-impact-assessments/ (accessed June 18, 2020) ("OPC privacy impact assessments").

PIPEDA, *Breach of Security Safeguards Regulations*, SOR/2018-64, effective November 1, 2018, online: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2018-64/index.html ("PIPEDA, *Breach of Security Safeguards Regulations*").

"PIPEDA fair information principles", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/ (accessed 21 May 2020) ("PIPEDA fair information principles").

"PIPEDA in brief", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (accessed 21 May 2020) ("OPC PIPEDA in brief").

"Privacy 101 presentation ", OPC, online: https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/pp_101/ (accessed 20 May 2020) ("OPC privacy 101 presentation").

"Privacy and the COVID-19 outbreak", OPC, March 2020, online: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/ ("Privacy and the COVID-19 outbreak, March 2020" or "March 2020 OPCC COVID-19 Privacy Guidance").

"Privacy law reform – a pathway to respecting rights and restoring trust in government and the digital economy: 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act", OPC, December 10, 2019, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/ ("OPCC Annual Report" or "OPC 2018-2019 Report to Parliament on Privacy Act and PIPEDA").

"Privacy review of the COVID Alert exposure notification application", OPC, July 31, 2020 https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/ ("OPCC: Privacy review of the COVID Alert exposure notification application").

"Provincial laws that may apply instead of PIPEDA", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/ (accessed 21 May 2020) ("OPC: Provincial laws that may apply instead of PIPEDA").

"Speaking notes for a general audience", OPC, online: https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/pp_101_notes/ (accessed 20 May 2020) ("OPC: Speaking notes for a general audience").

"Summary of privacy laws in Canada", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ (last revised January 2018; accessed May 20 and June 12, 2020) ("OPCC summary of privacy laws in Canada" or "OPC summary of privacy laws in Canada").

"The federal government and your personal information", OPC, online: https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/the-federal-government-and-your-personal-information/ (accessed 21 May 2020) ("OPC: The federal government and your personal information").

"Top ten dos and don'ts for privacy impact assessments", OPC, online: https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_59_pia/ (accessed June 18, 2020) ("Top ten dos and don'ts for privacy impact assessments").

"What to consider when reading a privacy policy", OPC, online: https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/02_05_d_71_pp/ (accessed 20 May 2020) ("OPC: What to consider when reading a privacy policy")

"What you need to know about mandatory reporting of breaches of security safeguards", OPC, October 29, 2018, online: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/ (accessed July 21, 2020) ("OPCC Mandatory Breach Reporting Guidance").

PT PRIVACY COMMISSIONERS

OVERALL

N/A

ALBERTA OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER ("AB OIPC" OR "AB PRIVACY COMMISSIONER")

"Commissioner releases report on ABTraceTogether contact-tracing app", Alberta OIPC, July 9, 2020, online: https://www.oipc.ab.ca/news-and-events/news-releases/2020/commissioner-releases-report-on-abtracetogether-contact-tracing-app.aspx ("Commissioner releases report on ABTraceTogether contact-tracing app").

"Privacy impact assessment", Alberta OIPC, online: https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx ("Alberta OIPC: Privacy impact assessment").

"Privacy impact assessment requirements", Alberta OIPC, online: https://www.oipc.ab.ca/media/615916/Guide_PIA_Requirements_2010.pdf ("Alberta OIPC: Privacy impact assessment requirements").

"Privacy in a pandemic", Alberta OIPC, March 2020, online: https://www.oipc.ab.ca/resources/privacy-in-a-pandemic-advisory.aspx ("Alberta OIPC: Privacy in a pandemic").

BC OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER ("BC OIPC" OR "BC PRIVACY COMMISSIONER")

"BC Information and Privacy Commissioner's statement on COVID-19", March 16, 2020, online: https://www.oipc.bc.ca/news-releases/2396 ("BC Privacy Commissioner's statement on COVID-19").

MB OFFICE OF THE OMBUDSMAN ("MB PRIVACY COMMISSIONER")

"Longer extensions under FIPPA: advisory for public bodies about extensions under FIPPA during the COVID-19 pandemic", online: https://www.ombudsman.mb.ca/info/longer-extensions-under-fippa.html ("MB Privacy Commissioner: longer extensions under FIPPA")

NB OFFICE OF THE OMBUDSMAN ("NB OMBUDSMAN" OR "NB PRIVACY COMMISSIONER")

"Guidance: privacy in emergency situations" (also referred to as "Guidance document on the protection of privacy and the outbreak of COVID-19"), March 27, 2020, online: https://ombudnb-aip-aivp.ca/wp-content/uploads/2020/05/Guidance-Privacy-in-Emergency-Situations-Eng.pdf ("NB Privacy Commissioner Guidance: privacy in emergency situations").

NL + LD OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER ("NL + LD OIPC" OR "NL + LD PRIVACY COMMISSIONER")

"Don't blame privacy – what to do and how to communicate in an emergency", updated April 2020, online: https://www.oipc.nl.ca/pdfs/EmergenciesPrivacy.pdf ("NL + LD Privacy Commissioner: Don't blame privacy").

NWT INFORMATION AND PRIVACY COMMISSIONER ("NWT OIPC" OR "NWT PRIVACY COMMISSIONER")

"Privacy in a pandemic", March 2020, online: https://atipp-nt.ca/wp-content/uploads/2020/03/Privacy-in-a-Pandemic.pdf ("NWT OIPC: Privacy in a pandemic").

NS INFORMATION AND PRIVACY COMMISSIONER ("NS PRIVACY COMMISSIONER")

"Nova Scotia's Information and Privacy Commissioner's statement on COVID-19", March 24, 2020, online: https://oipc.novascotia.ca/sites/default/files/Press-Releases/2020%2003%2024_Public%20message%20re%20covid-19.pdf ("Nova Scotia Privacy Commissioner's statement on COVID-19").

NU INFORMATION AND PRIVACY COMMISSIONER ("NU PRIVACY COMMISSIONER")

N/A

ON INFORMATION AND PRIVACY COMMISSIONER ("ON OIPC" OR "ONTARIO PRIVACY COMMISSIONER")

"Impact of COVID-19", Ontario OIPC, March 16, 2020, updated June 26, 2020, online: https://www.ipc.on.ca/newsrelease/ipc-closure-during-covid-19-outbreak/ ("Ontario OIPC: Impact of COVID-19").

"Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert", July 30, 2020, https://www.ipc.on.ca/wp-content/uploads/2020/07/2020-07-30-ltr-michael-maddock-re-ipc-recommendations-to-the-government-of-ontario-regarding-covid-alert.pdf ("Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert").

PEI INFORMATION AND PRIVACY COMMISSIONER ("PEI PRIVACY COMMISSIONER")

N/A

QC COMMISSION D'ACCÈS À L'INFORMATION ("QC PRIVACY COMMISSIONER")

"COVID-19: Protection des renseignements personnels et sécurité de l'information", March 25, 2020, online: https://www.cai.gouv.qc.ca/pandemie-de-covid-19-protection-des-renseignements-personnels-et-securite-de-linformation/ ("QC Privacy Commissioner – COVID-19: Protection des renseignements personnels et sécurité de l'information").

SK INFORMATION AND PRIVACY COMMISSIONER ("SK PRIVACY COMMISSIONER")

"Updated Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on COVID-19", April 20, 2020, online: https://oipc.sk.ca/statement-from-the-office-of-the-information-and-privacy-commissioner-of-saskatchewan-on-covid-19/ ("Updated Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on COVID-19").

YK OMBUDSMAN AND INFORMATION AND PRIVACY COMMISSIONER ("YK PRIVACY COMMISSIONER")

"Actions being taken by Yukon Ombudsman, Information and Privacy Commissioner and Public Interest Disclosure Commissioner in response to COVID-19 - Updated March 18 2020", online: https://www.ombudsman.yk.ca/news/view/115/32 ("Actions being taken by Yukon Ombudsman, Information and Privacy Commissioner and Public Interest Disclosure Commissioner in response to COVID-19 - Updated March 18 2020").

COURTS

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

GOVERNMENT – FOREIGN

SUPRANATIONAL

EUROPEAN UNION ("EU")

EHEALTH NETWORK (EUROPEAN COMMISSION)

"eHealth network guidelines to the EU member states and the European Commission on interoperability specifications for cross-border transmission chains between approved apps", European Commission, eHealth Network, June 12, 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf ("EC: eHealth network guidelines to the EU member states and the European Commission on interoperability specifications for cross-border transmission chains between approved apps").

"Interoperability guidelines for approved contact tracing mobile applications in the EU", European Commission, eHealth Network, May 13, 2020, online: https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf ("EC: Interoperability guidelines for approved contact tracing mobile applications in the EU").

"Mobile applications to support contact tracing in the EU's fight against COVID-19 - common EU toolbox for Member States", European Commission, eHealth Network, April 15, 2020, online: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf ("EC: Mobile applications to support contact tracing in the EU's fight against COVID-19 - common EU toolbox for Member States").

EUROPEAN COMMISSION ("EC") & EUROPEAN PARLIAMENT

"Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU", European Commission, Press Release, May 19, 2020, online: https://ec.europa.eu/eip/ageing/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu_en ("EC - Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU").

"Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures", European Commission, Press release, April, 16, 2020, online: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670 ("EC - Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures").

"Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps", European Commission, Press release, April 8, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626 ("EC - Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps").

"Digital technologies – innovative solutions during the coronavirus crisis", European Commission, online: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/digital_en ("EC: Digital technologies – innovative solutions during the coronavirus crisis").

"Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection", European Commission, Brussels, 16.4.2020 C(2020) 2523 final ("EC Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection").

"Joint European roadmap towards lifting COVID-19 containment measures", European Parliament and European Commission, April 15, 2020, online: https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf ("EP & EC Joint European roadmap towards lifting COVID-19 containment measures" or "EU exit strategy roadmap").

EUROPEAN DATA PROTECTION BOARD ("EDPB")

Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, EDPB, April 21, 2020, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf ("EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak").

Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, EDPB, April 21, 2020, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf ("EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak").

"Statement on the data protection impact of the interoperability of contact tracing apps", Adopted on 16 June 2020, EDPB, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf ("EDPB statement on App Interoperability").

"Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak", Adopted on 16 June 2020, EDPB, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementreopeningbordersanddataprotection_en.pdf ("EDPB statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak").

"Thirty-second plenary session: Statement on the interoperability of contact tracing applications, statement on the opening of borders and data protection rights, response letters to MEP Körner on laptop camera covers and encryption and letter to the Commi", EDPB News Release, June 17, 2020, online: https://edpb.europa.eu/news/news/2020/thirty-second-plenary-session-statement-interoperability-contact-tracing-0_en ("EDPB news release re: statement on the interoperability of contact tracing applications").

WORLD HEALTH ORGANIZATION ("WHO")

"Contact tracing in the context of COVID-19 (Interim Guidance)", WHO, May 10, 2020, online: https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19 ("WHO: Contact tracing in the context of COVID-19 [Interim Guidance]").

"Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19", WHO, June 2, 2020, online: file:///Users/Deborah/Downloads/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1-eng.pdf ("WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 [Interim Guidance]").

NATIONAL

FRANCE

COMMISSION NATIONALE INFORMATIQUE & LIBERTES ("CNIL")

"Opinion on the draft decree regarding the conditions for the implementation of the StopCovid app", CNIL, May 26, 2020, online: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf ("CNIL Opinion on the draft decree regarding the conditions for the implementation of the StopCovid app").

"The CNIL gives its opinion on the conditions for implementing the 'StopCovid' application", CNIL News Release (Translated from French), May 26, 2020, https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid ("The CNIL gives its opinion on the conditions for implementing the 'StopCovid' application").

UNITED KINGDOM ("UK")

UK GOVERNMENT

"Keeping workers and customers safe during COVID-19 in restaurants, pubs, bars and takeaway services: COVID-19 secure guidance for employers, employees and the self-employed", UK Government, June 23, 2020, online: https://assets.publishing.service.gov.uk/media/5eb96e8e86650c278b077616/Keeping-workers-and-customers-safe-during-covid-19-restaurants-pubs-bars-takeaways-230620.pdf ("UK Government: Keeping workers and customers safe during COVID-19 in restaurants, pubs, bars and takeaway services: COVID-19 secure guidance for employers, employees and the self-employed").

UK NATIONAL CYBER SECURITY CENTRE

"The security behind the NHS contact tracing app", National Cyber Security Centre (Ira Levy), May 4, 2020, online: https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app ("The security behind the NHS contact tracing app").

NON-GOVERNMENT

A

"A data leak exposed the personal information of over 3,000 ring users", Buzzfeed News, December 19, 2019, online: https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users ("A data leak exposed the personal information of over 3,000 ring users").

"A flood of coronavirus apps are tracking us. Now it's time to keep track of them", MIT Technology Review, May 7, 2020, online: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ ("A flood of coronavirus apps are tracking us").

"A new data governance model for contact tracing: authorized public purpose access", World Economic Forum, August 12, 2020, online: https://www.weforum.org/agenda/2020/08/contact-tracing-apps-privacy-framework-appa-data-governance/ ("A new data governance model for contact tracing: authorized public purpose access").

"A typology of privacy", B. Koops et al, Penn Law: Legal Scholarship Repository, 2017, online: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi? article=1938&context=jil ("A typology of privacy").

"About Shopify", Shopify, online: https://www.shopify.ca/about (accessed June 1, 2020) ("About Shopify").

"About the Exposure Notification API update", Google, online: https://support.google.com/android/answer/9991216?p=exposure_notifications_update&visit_id=637313787104229467-1786682678&rd=1 (accessed July 26, 20200) ("Google - About the Exposure Notification API update").

"AccessPrivacy podcast: special thought leadership roundtable on privacy and the COVID-19 pandemic", Mondaq, May 27, 2020, online: https://www.mondaq.com/canada/privacy-protection/961018/accessprivacy-podcast-special-thought-leadership-roundtable-on-privacy-and-the-covid-19-pandemic ("AccessPrivacy podcast: special thought leadership roundtable on privacy and the COVID-19 pandemic").

"After COVID-19, will we live in a Big Brother world?", Cigi, June 1, 2020, online: https://www.cigionline.org/articles/after-covid-19-will-we-live-big-brother-world ("After COVID-19, will we live in a Big Brother world?").

"Alberta to adopt national COVID-19 exposure app", Globe & Mail, August 8-9, 2020 ("Alberta to adopt national COVID-19 exposure app").

"Alberta reports 49 new COVID-19 cases, one additional death", CBC News, June 18, 2020, online: https://www.cbc.ca/news/canada/edmonton/alberta-reports-49-new-covid-19-cases-one-additional-death-1.5618184 ("Alberta reports 49 new COVID-19 cases, one additional death").

"Alberta will switch over to national coronavirus tracing app", Global News, August 9, 2020, online: https://globalnews.ca/news/7261467/alberta-will-switch-over-to-national-coronavirus-contact-tracing-app/ ("Alberta will switch over to national coronavirus tracing app").

"Amazon refuses blame for Capital One data breach, says its cloud services were 'not compromised in any way'", Newsweek, July 30, 2019, online: https://www.newsweek.com/amazon-capital-one-hack-data-leak-breach-paige-thompson-cybercrime-1451665 ("Amazon refuses blame for Capital One data breach, says its cloud services were 'not compromised in any way'").

"And the Littlest State Shall Lead the Way on Covid-19", Bloomberg, July 13, 2020 ("And the Littlest State Shall Lead the Way on Covid-19").

"Android 11 release date: when can you expect it to launch?", Android Authority (Jimmy Westenberg), August 6, 2020, online: www.androidauthority .com/android-11-release-date-1085250/ ("Android 11 release date: when can you expect it to launch?").

"Anonymization by decentralization? The case of COVID-19 contact tracing apps", S. Rossello and P Dewitte, European Law Blog, May 25, 2020, online: https://europeanlawblog.eu/2020/05/25/anonymization-by-decentralization-the-case-of-covid-19-contact-tracing-apps/ ("Anonymization by decentralization? The case of COVID-19 contact tracing apps").

"Apple's empty grandstanding about privacy", The Atlantic, January 31, 2019, online: https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ ("Apple's empty grandstanding about privacy").

"Apple, Google Covid-19 tool to be limited to one app per country", Bloomberg, May 4, 2020, online: https://www.bloomberg.com/news/articles/2020-05-04/apple-google-covid-19-tool-to-be-limited-to-one-app-per-country?utm_source=The+Logic+Master+List&utm_campaign=af8e730135-Daily_Briefing_2020_June22_2&utm_medium=email&utm_term=0_325d5d3b52-af8e730135-275653649 ("Apple, Google Covid-19 tool to be limited to one app per country").

"Apple, Google In Conflict With States Over Contact-Tracing Tech", npr.org, May 13, 2020 ("Apple, Google In Conflict With States Over Contact-Tracing Tech").

"Apple, Google release their joint technology for pandemic-tracking apps", cbc.ca, May 20, 2020 ("Apple, Google release their joint technology for pandemic-tracking apps").

"Apple and Google's exposure notification system now publicly available", Mobile Syrup, May 20, 2020 ("Apple and Google's exposure notification system now publicly available").

"Apple and Google roll out their new exposure notification tool. Interest seems limited", Recode, May 20, 2020, online: https://www.vox.com/recode/2020/5/20/21264045/apple-google-exposure-notification-contact-tracing-release ("Apple and Google roll out their new exposure notification tool. Interest seems limited").

"Applications of digital technology in COVID-19 pandemic planning and response", The Lancet Digital Health, June 29, 2020, online: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30142-4/fulltext ("Applications of digital technology in COVID-19 pandemic planning and response").

"Are contact-tracing apps helping tame the pandemic?", livemint, August 5, 2020, online: https://www.livemint.com/news/india/are-contact-tracing-apps-helping-tame-the-pandemic-11596611635201.html ("Are contact-tracing apps helping tame the pandemic?").

"As debate over contact tracing continues, CSE warns of foreign surveillance technology", CBC News, May 26-27, 2020 ("As debate over contact tracing continues, CSE warns of foreign surveillance technology").

"Assess privacy before launching contact tracing apps, advocacy groups say", The Wire Report, June 24, 2020 ("Assess privacy before launching contact tracing apps, advocacy groups say").

"At Mayo Clinic, sharing patient data with companies fuels AI innovation – and concerns about consent", Stat News, June 3, 2020 ("At Mayo Clinic, sharing patient data with companies fuels AI innovation – and concerns about consent").

B

"Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy", Amnesty International, June 16, 2020, online: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ ("Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy").

"BC contact-tracing app tackles Canadians' privacy concerns", Prince George Matters, May 31, 2020, online: https://www.princegeorgematters.com/local-news/bc-contact-tracing-app-tackles-canadians-privacy-concerns-2398577 ("BC contact-tracing app tackles Canadians' privacy concerns").

"Big tech in healthcare: here's who wins and loses as Alphabet, Amazon, Apple, and Microsoft hone in on niche sectors of healthcare", Business Insider, January 30, 2020, online: https://www.businessinsider.com/big-tech-in-healthcare-report ("Big tech in healthcare: here's who wins and loses as Alphabet, Amazon, Apple, and Microsoft hone in on niche sectors of healthcare").

"Big Three want CRTC to dismiss PIAC's contact-tracing demand", cartt.ca, May 12, 2020 ("Big Three want CRTC to dismiss PIAC's contact-tracing demand").

"Big Tech's power, in 4 numbers", Axios, July 27, 2020 ("Big Tech's power, in 4 numbers").

"Blackberry and how automotive AI could revolutionize healthcare", *Datamation* (Rob Enderle), April 24, 2020, online: www.datamation.com/artificial-intelligence/blackberry-and-how-automotive-ai-could-revolutionize-healthcare.html ("Blackberry and how automotive AI could revolutionize healthcare").

"BlackBerry CEO says the mobile company's turnaround has hit a tipping point after near-death experience", CNBC Evolve (Joel Dreyfuss), September 14, 2019, online: www.cnbc.com/2019/09/14/blackberry-ceo-says-hes-hit-tipping-point-in-company-turnaround.html ("BlackBerry CEO says the mobile company's turnaround has hit a tipping point after near-death experience").

"BlackBerry Healthcare Momentum Continues with Latest HIMSS INFRAM Certification", BlackBerry ThreatVector Blog, November 29, 2018, online: blogs.blackberry.com/en/2018/11/blackberry-healthcare-momentum-continues-with-latest-himss-infram-certification ("BlackBerry healthcare momentum continues with latest HIMSS INFRAM certification").

"BlackBerry Solutions for Healthcare Providers", BlackBerry, online: www.blackberry.com/us/en/industries/healthcare ("BlackBerry solutions for healthcare providers").

"Bluetooth contact tracing apps built with Google and Apple's APIs still collect Android users' location data", mobihealthnews, July 21, 2020 ("Bluetooth contact tracing apps built with Google and Apple's APIs still collect Android users' location data").

"Bogus 'contact tracing' apps deployed to steal data: researchers", CTV news, June 10, 2020, online: https://www.ctvnews.ca/sci-tech/bogus-contact-tracing-apps-deployed-to-steal-data-researchers-1.4978348 ("Bogus 'contact tracing' apps deployed to steal data: researchers").

"Bracelets, beacons, barcodes: wearables in the global response to COVID-19", Electronic Frontier Foundation ("EFF"), June 16, 2020, online: https://ifex.org/bracelets-beacons-barcodes-wearables-in-the-global-response-to-covid-19/ ("Bracelets, beacons, barcodes: wearables in the global response to COVID-19").

"Bridging the gaps: a path forward to federal privacy legislation", Report, Brookings (C. F. Kerry et al), June 3, 2020, online: https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf ("Brookings Report, Bridging the gaps: a path forward to federal privacy legislation").

"Bugs force Japan gov't to temporarily shut down virus contact-tracing app", Kyodo News, June 23, 2020, online: https://english.kyodonews.net/news/2020/06/eefc1a227d7e-bugs-force-govt-to-temporarily-shut-down-virus-contact-tracing-app.html?utm_source=The+Logic+Master+List&utm_campaign=4529c36237-Daily_Briefing_2020_June23_2&utm_medium=email&utm_term=0_325d5d3b52-4529c36237-275653649 ("Bugs force Japan gov't to temporarily shut down virus contact-tracing app").

"Businesses face privacy minefield over contact-tracing rules, say campaigners", The Guardian, June 24, 2020, online: https://www.theguardian.com/technology/2020/jun/24/businesses-face-privacy-minefield-contact-tracing-rules-england-campaigners ("Businesses face privacy minefield over contact-tracing rules, say campaigners").

C

"Canada: amendments to Ontario's health information legislation bring new obligations and penalties", Mondaq (McCarthy Tetrault), June 24, 2020, online: https://www.mondaq.com/canada/privacy-protection/957346/amendments-to-ontario39s-health-information-legislation-bring-new-obligations-and-penalties ("Canada: amendments to Ontario's health information legislation bring new obligations and penalties").

"Canada: balancing privacy and convenience: medical information and the emergence of virtual medicine", Mondaq (Bennett Jones LLP), June 25, 2020, online: https://www.mondaq.com/canada/privacy-protection/958302/balancing-privacy-and-convenience-medical-information-and-the-emergence-of-virtual-medicine ("Canada: balancing privacy and convenience: medical information and the emergence of virtual medicine").

"Canada: COVID-19 contact tracing debate highlights need for privacy law reform: lessons for developers and users", Mondaq (Miller Thomson LLP), June 16, 2020, online: https://www.mondaq.com/canada/operational-impacts-and-strategy/953516/covid-19-contact-tracing-debate-highlights-need-for-privacy-law-reform-lessons-for-developers-and-users ("Canada: COVID-19 contact tracing debate highlights need for privacy law reform: lessons for developers and users").

"Canada: Cybersecurity Comparative Guide", Mondaq, INQ Data Law (Carole Piovesan), July 7, 2020 ("Canada: Cybersecurity Comparative Guide").

"Canada: legal responses to health emergencies", Library of Congress Law, February 2015, online: https://www.loc.gov/law/help/health-emergencies/canada.php ("Canada: legal responses to health emergencies").

"Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC", Mondaq (S Pinsky & P Brown), June 8, 2020, online: https://www.mondaq.com/canada/privacy-protection/949554/modernizing-federal-privacy-laws-suggested-approaches-of-the-federal-government-and-the-opc?signup=true ("Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC").

"Canada: Ontario government to launch COVID Alert, a contact tracing app, in July", Mondaq (Bereskin & Parr), June 23, 2020, online: https://www.mondaq.com/canada/operational-impacts-and-strategy/956994/ontario-government-to-launch-covid-alert-a-contact-tracing-app-in-july ("Canada: Ontario government to launch COVID Alert, a contact tracing app, in July").

"Canada: privacy protection in Quebec: an overview of amendments to the law governing the private sector", Mondaq, Langlois lawyers, LLP (Jean-François De Rico , Caroline Deschênes , Pascal Archambault and Justine Brien), July 8, 2020 ("Canada: privacy protection in Quebec: an overview of amendments to the law governing the private sector").

"Canada: Quebec introduces new amendments to its privacy regimes", Mondaq, Blake, Cassels & Graydon LLP (Imran Ahmad , Marie-Hélène Constantin , Sunny Handa and Joe Abdul-Massih), June 17, 2020 ("Canada: Quebec introduces new amendments to its privacy regimes").

"Canada: the ABTraceTogether app – key privacy considerations", Mondaq (Field LLP), June 2, 2020, online: https://www.mondaq.com/canada/privacy-protection/945366/the-abtracetogether-app--key-privacy-considerations ("Canada: the ABTraceTogether app – key privacy considerations").

"Canada-US border will remain closed until September 21", CBC News, August 14, 2020, online: https://www.cbc.ca/news/politics/canada-us-border-closure-september-21-1.5686475 ("Canada-US border will remain closed until September 21").

"Canada's coronavirus cases pass 120,000 as global total reaches 20 million", Global News, August 10, 2020, online: https://globalnews.ca/news/7264520/canada-coronavirus-august-20/ ("Canada's coronavirus cases pass 120,000 as global total reaches 20 million").

"Canada has an army of volunteers ready to help fight COVID-19 – so why aren't we using them?", CBC, June 6, 2020, online: https://www.cbc.ca/news/health/covid19-canada-volunteers-1.5600484 ("Canada has an army of volunteers ready to help fight COVID-19 – so why aren't we using them?")

"Canada, U.S. attorneys general discussed law to speed up police access to data across borders", The Logic, June 12, 2020 ("Canada, U.S. attorneys general discussed law to speed up police access to data across borders").

"Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act", The Globe & Mail, June 25, 2020, online: https://www.theglobeandmail.com/canada/investigations/article-canadas-lost-months-when-covid-19s-first-wave-hit-governments-and/ ("Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act").

"Canada's new COVID app won't work on older iPhones, Android devices", CP24, August 3, 2020, online: https://www.cp24.com/news/canada-s-new-covid-app-won-t-work-on-older-iphones-android-devices-1.5049400 ("Canada's new COVID app won't work on older iPhones, Android devices").

"Canada's out-of-date online privacy rules aren't protecting you", The Conversation, July 26, 2020, online: https://theconversation.com/canadas-out-of-date-online-privacy-rules-arent-protecting-you-142585 ("Canada's out-of-date online privacy rules aren't protecting you")

"Canada's population has grown to nearly 38 million: Stats Can", Daily Hive, July 13, 2020, online: https://dailyhive.com/vancouver/population-of-canada-statistics-38-million ("Canada's population has grown to nearly 38 million: Stats Can").

"Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps", CBC, May 8, 2002, online: https://www.cbc.ca/news/canada/new-brunswick/covid-19-contact-tracing-app-privacy-commissioners-new-brunswick-1.5557548 ("Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps").

"Canada's privacy watchdogs see uptick in work amid pandemic", The Logic, July 30, 2020 ("Canada's privacy watchdogs see uptick in work amid pandemic").

"Canada's proposed contact-tracing app takes the right approach on privacy", The Globe & Mail, June 18, 2020, online: https://www.theglobeandmail.com/opinion/article-canadas-proposed-contact-tracing-app-takes-the-right-approach-on/ ("Canada's proposed contact-tracing app takes the right approach on privacy").

"Canadian data privacy regulator releases guidance for Canadian privacy law compliance during COVID-19", Privacy & Data Security Law Blog, Winston & Strawn LLP, April 22, 2020 ("Canadian data privacy regulator releases guidance for Canadian privacy law compliance during COVID-19").

"Canadian government breaches exposed citizens' data: report", Bank Info Security, February 19, 2020, online: https://www.bankinfosecurity.com/canadian-government-breaches-exposed-citizens-data-report-a-13739 ("Canadian government breaches exposed citizens' data: report").

"Canadian health officials using Uber data to track COVID-19", The Logic, July 21, 2020 ("Canadian health officials using Uber data to track COVID-19").

"Canadian privacy watchdogs support COVID-19 exposure app", CTV News (Alexandra Mae Jones), August 3, 2020, online: www.ctvnews.ca/health/coronavirus/canadian-privacy-watchdogs-support-covid-19-exposure-app-1.5049847 ("Canadian privacy watchdogs support COVID-19 exposure app").

"Canadians' security and privacy must be protected in the race to trace", Ryerson University, Cybersecure Policy Exchange ("CPE"), June 8, 2020, online: https://www.newswire.ca/news-releases/canadians-security-and-privacy-must-be-protected-in-the-race-to-trace-862465542.html ("Canadians' security and privacy must be protected in the race to trace").

"Can't download the COVID Alert app? Your operating system may be too old (or new)", Global News, August 2, 2020, online: https://globalnews.ca/news/7244628/coronavirus-covid-alert-app-download/ ("Can't download the COVID Alert app? Your operating system may be too old (or new)").

"Care19 Alert", North Dakota government, online: https://ndresponse.gov/covid-19-resources/care19 ("Care19 Alert").

"Carly Kind on contact-tracing apps", Big Tech (podcast), June 4, 2020 ("Carly Kind on contact-tracing apps").

"Chapter 7: Canada", Osler, Hoskin & Harcourt LLP, in ICLG's *The International Comparative Guide to Data Protection 2018*, 5th edition, online: https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf ("Chapter 7: Canada, in *The International Comparative Guide to Data Protection 2018*").

"Commission won't investigate contact-tracing apps", cartt.ca, May 13, 2020 ("Commission won't investigate contact-tracing apps").

"Company announcements: an update on exposure notifications", Google: The Keyword (Dave Burke), July 31, 2020, online: blog.google/inside-google/company-announcements/update-exposure-notifications/ ("Company announcements: an update on exposure notifications").

"Contact tracing and a company's role as detective", Forbes, July 28, 2020, online https://www.forbes.com/sites/forbestechcouncil/2020/07/28/contact-tracing-and-a-companys-role-as-detective/#37ba19d179eb "Contact tracing and a company's role as detective").

"Contact-tracing apps are a job for multipartisan leadership", The Globe & Mail (Campbell Clark), June 19, 2020, online: https://www.theglobeandmail.com/politics/article-contact-tracing-apps-are-a-job-for-multipartisan-leadership/ ("Contact-tracing apps are a job for multipartisan leadership").

"Contact tracing apps in Canada: a new world for data privacy", Norton Rose Fulbright, May 11, 2020, online: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/canada-contact-tracing.pdf?revision=cb0f741a-377a-47c1-bd22-b3eb28f66fed&la=en-ca ("Contact tracing apps in Canada: a new world for data privacy").

"Contact tracing apps may help slow the spread of COVID-19. But will privacy concerns prevent Canadians from using them?", Toronto Star, June 22, 2020, online: https://www.thestar.com/business/2020/06/22/contact-tracing-apps-may-help-slow-the-spread-of-covid-19-but-will-privacy-concerns-prevent-canadians-from-using-them.html ("Contact tracing apps may help slow the spread of COVID-19. But will privacy concerns prevent Canadians from using them?").

"Contact tracers in England get no data from 26% of people with coronavirus", The Guardian, June 18, 2020, online: https://www.theguardian.com/world/2020/jun/18/contact-tracers-in-england-get-no-data-from-26-of-people-with-coronavirus ("Contact tracers in England get no data from 26% of people with coronavirus").

"Contact tracing and privacy: we need both to restart the economy and get employees back to work", PwC (Jordan Prokopy and John B. Simcoe), on or around July 11, 2020, online: https://www.pwc.com/ca/en/industries/telecommunications/contact-tracing-and-privacy-restart-economy-to-get-employees-back-to-work.html ("Contact tracing and privacy: we need both to restart the economy and get employees back to work").

"Contact tracing information at Ontario bars, restaurants raises privacy concerns", iheartradio.ca, August 4, 2020 ("Contact tracing information at Ontario bars, restaurants raises privacy concerns").

"Contact tracing must not compound historical discrimination", Policy Options (Chris Parsons), April 30, 2020, online: https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/ ("Contact tracing must not compound historical discrimination").

"Contact tracing with your phone: it's easier but there are tradeoffs", New York Times, June 3, 2020, https://www.nytimes.com/2020/06/03/health/ coronavirus-contact-tracing-apps.html?utm_source=The+Logic+Master+List&utm_campaign=4657f6904c-Daily_Briefing_2020_June4_

2&utm_medium=email&utm_term=0_325d5d3b52-4657f6904c-275653649 ("Contact tracing with your phone: it's easier but there are tradeoffs").

"Continuously improving COVID Alert", Canadian Digital Service ("CDS") Blog (Josh Ruihley, Emily Kuret, Stephen Yates, Courtney Claessens, & Sean Boots), July 31, 2020, online: digital.canada.ca/2020/07/31/continuously-improving-covid-alert/ ("Continuously improving COVID Alert").

"Coronavirus: does anyone have a working contact-tracing app?", BBC, June 25, 2020, online: https://www.bbc.com/news/53168438 ("Coronavirus: does anyone have a working contact-tracing app?").

"Coronavirus: feds mum on launch date for contact-tracing app after Ontario pilot delayed", Global News, July 22, 2020, online: https://globalnews.ca/news/7200520/coronavirus-feds-mum-date-contact-tracing-app/ ("Coronavirus: feds mum on launch date for contact-tracing app after Ontario pilot delayed").

"Coronavirus: how much does your boss need to know about you?", BBC News, June 30, 2020, online: https://www.bbc.com/news/business-53109207 ("Coronavirus: how much does your boss need to know about you?").

"Coronavirus: the great contact-tracing apps mystery", BBC News, July 22, 2020, online: https://www.bbc.com/news/technology-53485569 ("Coronavirus: the great contact-tracing apps mystery").

"Coronavirus: Why Singapore turned to wearable contact-tracing tech", BBC, July 5, 2020, online: https://www.bbc.com/news/technology-53146360 ("Coronavirus: Why Singapore turned to wearable contact-tracing tech").

"Coronavirus app warning: StopCovid collects data of ANYONE near user in major system fault", Daily Express, June 17, 2020, online: https://www.express.co.uk/news/world/1297160/coronavirus-app-tracking-cases-latest-data-breach-warning-stopcovid-app-trace-France

"Coronavirus contact-tracing: world split between two types of app", BBC, May 7, 2020, online: https://www.bbc.com/news/technology-52355028 ("Coronavirus contact-tracing: world split between two types of app").

"Coronavirus contact-tracing app to launch nationally in early July, Trudeau says", Global News, June 18, 2020, online: https://globalnews.ca/news/7079851/coronavirus-tracing-app-launch-nationally/ ("Coronavirus contact-tracing app to launch nationally in early July, Trudeau says").

"Coronavirus contact tracing apps were tech's chance to step up. They haven't.", NBC News, June 12, 2020, online: https://www.nbcnews.com/tech/tech-news/coronavirus-contact-tracing-apps-were-tech-s-chance-step-they n1230211?utm_source=The+Logic+Master+List&utm_campaign= 517c6e4fb4-Daily_Briefing_2020_June12_2&utm_medium=email&utm_term=0_325d5d3b52-517c6e4fb4-275653649 ("Coronavirus contact tracing apps were tech's chance to step up").

"Coronavirus, invisible threats and preparing for resilience", Gunhild Hoogensen Gjørv, NATO Review, May 20, 2020, online: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html ("Coronavirus, invisible threats and preparing for resilience").

"Coronavirus statement", University of Waterloo Cybersecurity and Privacy Institute, May 19, 2020, online: https://uwaterloo.ca/cybersecurity-privacy-institute/news/coronavirus-statement ("Coronavirus statement").

"Coronavirus tracing app a test for privacy-minded Germany", ABC News, June 16, 2020, online: https://abcnews.go.com/Health/wireStory/coronavirus-tracing-app-test-privacy-minded-germany-71270334 ("Coronavirus tracing app a test for privacy-minded Germany").

"Coronavirus tracing app not yet OK'd by privacy watchdog, but outside experts give thumbs up", Global News, June 18, 2020, online: https://globalnews.ca/news/7081057/coronavirus-tracing-app-privacy-watchdog-experts/ ("Coronavirus tracing app not yet OK'd by privacy watchdog, but outside experts give thumbs up").

Could this COVID-19 'health passport' be the future of travel and events?", World Economic Forum, July 30, 2020, online: https://www.weforum.org/agenda/2020/07/covid-19-passport-app-health-travel-covidpass-quarantine-event/ ("Could this COVID-19 'health passport' be the future of travel and events?")

"COVI White Paper – Version 1.0", Mila, May 18, 2020, online: https://mila.quebec/wp-content/uploads/2020/05/COVI-whitepaper-V1.pdf ("COVI White Paper – Version 1.0").

"COVID Alert app could result in some people being ID'd", CBC News, August 5, 2020 ("COVID Alert app could result in some people being ID'd").

"COVID Alert app one of many tools in fight against coronavirus, Dr. Tam says", Globe & Mail, August 4, 2020 ("COVID Alert app one of many tools in fight against coronavirus, Dr. Tam says")

"COVID Alert, federally backed contact tracing app, hints at what Manitobans may be able to expect", CBC News, July 2, 2020, online: https://www.cbc.ca/news/canada/manitoba/manitoba-covid-19-contact-tracing-app-1.5632875 ("COVID Alert, federally backed contact tracing app, hints at what Manitobans may be able to expect")

"COVID Alert Portal for healthcare providers", Github, online: github.com/cds-snc/covid-alert-portal ("COVID Alert Portal for healthcare providers").

"COVID contact tracing has privacy concerns: security expert", Kitchener Today, May 21, 2020 ("COVID contact tracing has privacy concerns: security expert").

"Covid crisis changes no minds on MVNO question", cartt.ca, June 4, 2020 ("Covid crisis changes no minds on MVNO question").

"Covid Shield" (dedicated website), online: https://www.covidshield.app/ (accessed June 1, 2020) ("Covid Shield website").

"COVID Shield could be a positive first step for privacy", OpenMedia, June 18, 2020, online: https://openmedia.org/press/item/covid-shield-could-be-a-positive-first-step-for-privacy ("COVID Shield could be a positive first step for privacy").

"Covid Tracker app throws spotlight on Google data harvesting", Irish Times, July 30, 2020 ("Covid Tracker app throws spotlight on Google data harvesting").

"COVID-19: when EU tacking apps meet the pandemic, trust and privacy by design are the hosts", The National Law Review, May 20, 2020, online: https://www.natlawreview.com/article/covid-19-when-eu-tracking-apps-meet-pandemic-trust-and-privacy-design-are-hosts ("COVID-19: when EU tacking apps meet the pandemic, trust and privacy by design are the hosts").

"COVID-19 and cellphone surveillance", ABlawg (Joel Reardon, Emily Laidlaw, and Greg Hagen), April 16, 2020, online http://ablawg.ca/wp-content/uploads/2018/07/Blog_JR_EL_GH_COVID.pdf ("COVID-19 and cellphone surveillance").

"COVID-19 and contact-tracing apps in Canada", Bennett Jones LLP, May 12, 2020, online: https://www.bennettjones.com/Blogs-Section/COVID-19-and-Contact-Tracing-Apps-in-Canada ("COVID-19 and contact-tracing apps in Canada").

"COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic", McCarthy Tetrault LLP (Barry Sookman), April 14, 2020, online: https://www.mccarthy.ca/en/insights/blogs/techlex/covid-19-and-privacy-artificial-intelligence-and-contact-tracing-combatting-pandemic ("COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic").

"COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives", Bereskin & Parr (Amanda Branch), April 27, 2020, online: https://bereskinparr.com/doc/covid-19-and-privacy-federal-privacy-commissioner-publishes-framework-to-help-government-institution ("COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives").

"COVID-19 contact tracing app are coming to a phone near you. How will we know whether they work?", Science Magazine, May 21, 2020, online: https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how ("COVID-19 contact tracing app are coming to a phone near you. How will we know whether they work?").

"COVID-19 contact tracing must be ethical and responsible. Here's why", World Economic Forum, July 24, 2020, online: https://www.weforum.org/agenda/2020/07/why-covid-19-contact-tracing-must-be-efficient-effective-and-responsible/ ("COVID-19 contact tracing must be ethical and responsible. Here's why").

"COVID-19 exposure notification app now available", CTV News, July 31, 2020 ("COVID-19 exposure notification app now available")

"COVID-19 exposure notification using Bluetooth low energy", Google, online: https://blog.google/documents/66/Overview_of_COVID-19_Contact_Tracing_Using_BLE_1.pdf (accessed July 26, 2020) ("Google - COVID-19 exposure notification using Bluetooth low energy").

"COVID-19 impact: Canada's privacy commissioners outline guidance for governments and developers of contact tracing technology", Cassels, May 13, 2020, online: https://cassels.com/insights/covid-19-impact-canadas-privacy-commissioners-outline-guidance-for-governments-and-developers-of-contact-tracing-technology/ ("COVID-19 impact: Canada's privacy commissioners outline guidance for governments and developers of contact tracing technology").

"COVID-19 privacy protection bill introduced with bipartisan support", ars technica, June 2, 2020, online: https://arstechnica.com/tech-policy/2020/06/covid-19-privacy-protection-bill-introduced-with-bipartisan-support/?utm_brand=arstechnica&utm_source=twitter&utm_social-type=owned&utm_medium=social ("COVID-19 privacy protection bill introduced with bipartisan support").

"COVID-19 roundup: Ontario delays its virus exposure-notification app launch", The Logic, July 2, 2020 ("COVID-19 roundup: Ontario delays its virus exposure-notification app launch").

"COVID-19 tracing: a Quebec application 'ready in a few weeks'", La Presse, Jul 20, 2020 ("COVID-19 tracing: a Quebec application 'ready in a few weeks'").

"COVID-19 tracing app starts beta testing after three-week delay", July 23, 2020, CBC News, online: https://www.cbc.ca/news/politics/covid19-tracing-app-beta-testing-1.5660619 ("COVID-19 tracing app starts beta testing after three-week delay").

"Covid-19 tracking apps, or: how to deal with pandemic most unsuccessfully", About Intel: European Voices on Surveillance, June 3, 2020, online: https://aboutintel.eu/covid-digital-tracking/ ("Covid-19 tracking apps, or: how to deal with pandemic most unsuccessfully").

"Criminal Lawyers' Association position on digital COVID-19 contact tracing", Criminal Lawyers' Association ("CLA"), on or around June 4, 2020, online: https://criminallawyers.ca/criminal-lawyers-association-position-on-digital-covid-19-contact-tracing/#_ftn1 ("Criminal Lawyers' Association position on digital COVID-19 contact tracing").

"Cross-country checkup", The Logic:

- Cross-country checkup, July 9, 2020 ("Cross-country checkup, July 9, 2020")
- Cross-country checkup, July 8, 2020 ("Cross-country checkup, July 8, 2020")

"CRTC rejects request to hold contact-tracing inquiry", cartt.ca, May 13, 2020 ("CRTC rejects request to hold contact-tracing inquiry").

"Cumulative confirmed COVID-19 deaths", Our World in Data, August 10, 2020, online: https://ourworldindata.org/covid-deaths#what-is-the-total-number-of-confirmed-deaths ("Cumulative confirmed COVID-19 deaths").

"Cyber defence agency found over 1,500 'malicious' fake Canadian government COVID-19 websites", National Post, May 27, 2020 ("Cyber defence agency found over 1,500 'malicious' fake Canadian government COVID-19 websites").

D

"Data for good: leveraging TELUS data against COVID-19", Telus, online: https://www.telus.com/en/about/covid-19-updates/privacy-statement (accessed 20 May 2020) ("Data for good: leveraging TELUS data against COVID-19").

"Data privacy laws collide with contact tracing efforts; privacy is prevailing", Reuters.com, July 21, 2020 ("Data privacy laws collide with contact tracing efforts; privacy is prevailing").

"Data wars: why technology advocates believe privacy regulations need serious reform", Financial Post, June 20, 2020, online: https://business.financialpost.com/technology/data-wars-why-technology-advocates-believe-privacy-regulations-need-serious-reform?utm_term=Autofeed&utm_medium=Social&utm_source=Twitter#Echobox=1592647829 ("Data wars: why technology advocates believe privacy regulations need serious reform").

"Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19", Tech Crunch, June 5, 2020, online: https://techcrunch.com/2020/06/05/demonstrating-15-contact-tracing-and-other-tools-built-to-mitigate-the-impact-of-covid-19/ ("Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19").

"Despite Ontario delay, more provinces considering signing on with federal COVID Alert app", The Logic, July 27, 2020 ("Despite Ontario delay, more provinces considering signing on with federal COVID Alert app").

"Determine appropriate retention for network logs #199", John O'Brien (on GitHub COVID Alert Diagnosis Server), August 5, 2020, online: github.com/cds-snc/covid-alert-server/issues/199#issuecomment-669139650 ("Determine appropriate retention for network logs #199").

"Developers building new digital contact-tracing app hope it prevents a COVID-19 recurrence", Canadian Lawyer, April 28, 2020, online: https://www.canadianlawyermag.com/resources/practice-management/developers-building-new-digital-contact-tracing-app-hope-it-prevents-a-covid-19-recurrence/329099 ("Developers building new digital contact-tracing app hope it prevents a COVID-19 recurrence").

"Digital contact tracing: perspectives on approaches to COVID-19", Berkman Klein Centre for Internet & Society at Harvard University, June 25, 2020, online: https://cyber.harvard.edu/story/2020-06/digital-contact-tracing-perspectives-approaches-covid-19 ("Digital contact tracing: perspectives on approaches to COVID-19"), including "Is digital contact tracing over before it began?", Jonathan Zittrain, online: https://medium.com/berkman-klein-center/is-digital-contact-tracing-over-before-it-began-925c72036ee7 ("Is digital contact tracing over before it began?").

"Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown", Oxford University, April 16, 2020 ("Oxford Study").

"Digital contact tracing for pandemic response", Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies, Project Muse, Johns Hopkins University Press, June 17, 2020 ("Digital contact tracing for pandemic response").

"Discussion and outline of privacy and sociological concerns for CCTI iterations and features", Mila (Tyler Kolody), undated ("Discussion and outline of privacy and sociological concerns for CCTI iterations and features").

"Does Covid-19 contact tracing pose a privacy risk? Your questions, answered", Wired, April 17, 2020, online: https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/ ("Does Covid-19 contact tracing pose a privacy risk? Your questions, answered").

"Double-double tracking: How Tim Hortons knows where you sleep, work and vacation", Financial Post, June 12, 2020, online: https://business.financialpost.com/technology/tim-hortons-app-tracking-customers-intimate-data ("Double-double tracking: How Tim Hortons knows where you sleep, work and vacation").

E

"EDITORIAL: Are you up for the COVID contact-tracing app?", The Chronicle Herald, August 4, 2020, online: https://www.thechronicleherald.ca/opinion/local-perspectives/editorial-are-you-up-for-the-covid-contact-tracing-app-481239/ ("EDITORIAL: Are you up for the COVID contact-tracing app?")

"eHealth raises data, privacy, and clinical questions: experts", The Wire Report, August 5, 2020 ("eHealth raises data, privacy, and clinical questions: experts").

"Employer use of contact tracing apps: the good, the bad, and the regulatory", The National Law Review, July 7, 2020 ("Employer use of contact tracing apps: the good, the bad, and the regulatory").

"Empowering Citizens against Covid-19 with an ML-based and decentralized risk awareness app", Mila, May 1, 2020 ("Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app").

"England has started testing a contact tracing app – again", MIT Technology Review, August 13, 2020, online: https://www.technologyreview.com/2020/08/13/1006769/england-covid-contact-tracing-app-second-attempt/ ("England has started testing a contact tracing app – again").

"Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing – Interim Guidance", World Health Organization, May 28, 2020, online: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 ("WHO: Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing – Interim Guidance").

"Ethical guidelines for COVID-19 tracing apps", Nature.com, May 28, 2020 ("Ethical guidelines for COVID-19 tracing apps").

"EU ruling on US agreement may nudge Canada to update our privacy law: Cavoukian", IT World Canada, July 17, 2020, online: https://www.itworldcanada.com/article/eu-ruling-on-us-agreement-may-nudge-canada-to-update-our-privacy-law-cavoukian/433319 ("EU ruling on US agreement may nudge Canada to update our privacy law: Cavoukian").

"EU-US Privacy Shield invalid: Schrems II", Barry Sookman blog, July 16, 2020 ("EU-US Privacy Shield invalid: Schrems II").

"Europe faces privacy concerns with contact-tracing apps", IE Global Vistra (Paul Sutton), May 27, 2020, online: https://ieglobal.vistra.com/blog/2020/5/europe-faces-privacy-concerns-contact-tracing-apps?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration ("Europe faces privacy concerns with contact-tracing apps").

"Europe proves contact-tracing apps aren't a coronavirus cure-all", HuffPost, July 24, 2020, online: https://www.huffingtonpost.ca/entry/coronavirus-contact-tracing-apps-europe_n_5f194aaac5b6f2f6c9f1c8e9?ri18n=true (**"**Europe proves contact-tracing apps aren't a coronavirus cure-all").

"Europe's coronavirus smartphone contact tracing apps", August 5, 2020, Financial Post, https://financialpost.com/pmn/business-pmn/europes-coronavirus-smartphone-contact-tracing-apps ("Europe's coronavirus smartphone contact tracing apps").

"Europe's top court strikes down data-sharing deal with U.S.", The Logic, July 16, 2020 ("Europe's top court strikes down data-sharing deal with U.S.").

"Europeans Aren't Really Using COVID-19 Contact-Tracing Apps", Vice.com, July 21, 2020 ("Europeans aren't really using COVID-19 contact-tracing apps").

"European Union: COVID-19: protecting personal data – the new normal", Mondaq, Appleby (Peter Colegate , Richard Field , Andrew Jowett , Claire Milne , Malcolm Moller , Steven Rees Davies and Andrew Weaver Appleby) July 6, 2020 ("European Union: COVID-19: protecting personal data – the new normal").

"Experts say Sask could be more transparent with COVID-19 data without sacrificing privacy", CBC, June 3, 2020, online: https://www.cbc.ca/news/canada/saskatchewan/sask-data-sharing-1.5593961 ("Experts say Sask could be more transparent with COVID-19 data without sacrificing privacy").

"Experts warn Canadians to brace for a new era of cyberthreats", The Globe and Mail, January 2, 2020, online: https://www.theglobeandmail.com/business/article-experts-warn-canadians-to-brace-for-a-new-era-of-cyberthreats/ ("Experts warn Canadians to brace for a new era of cyberthreats").

"Exposure notification APIs addendum (to the Apple Developer Program License Agreement)", Apple, online: https://developer.apple.com/contact/ request/download/Exposure_Notification_Addendum.pdf (accessed July 26, 2020) ("Apple API Terms of Service").

"Exposure notification cryptography specification preliminary — subject to modification and extension April 2020 v1.1", Google, online: https://www.blog.google/documents/60/Exposure_Notification_-_Cryptography_Specification_v1.1.pdf (accessed July 26, 2020) ("Google - Exposure notification cryptography specification preliminary — subject to modification and extension April 2020 v1.1").

"Exposure notification: Diagnosis Server implementation", Github, online: github.com/cds-snc/covid-alert-server ("Exposure notification: Diagnosis Server implementation").

"Exposure notifications: using technology to help public health authorities fight COVID-19", Google, online: https://www.google.com/covid19/exposurenotifications/ (accessed July 26, 2020) ("Google - Exposure notifications: using technology to help public health authorities fight COVID-19").

F

"Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights", Amnesty International, November 21, 2019, online: https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/ ("Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights").

"Facebook exposed 87 million users to Cambridge Analytica", Wired, April 4, 2018, online: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/ ("Facebook exposed 87 Million users to Cambridge Analytica").

"Facedrive health receives media coverage for COVID-19 contact tracing app 'TraceSCAN'", Financial Post, June 1, 2020, online: https://business.financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/facedrive-health-receives-media-coverage-for-covid-19-contact-tracing-app-tracescan ("Facedrive health receives media coverage for COVID-19 contact tracing app 'TraceSCAN'").

Facedrive website, facedrive.com (accessed June 1, 2020) ("Facedrive website").

"Facedrive launches TraceSCAN Wearables pilot project in partnership with Labourers' International Union of North America (LiUNA)", Business Wire, July 29, 2020, online: https://www.businesswire.com/news/home/20200729005282/en/Facedrive-Launches-TraceSCAN-Wearables-Pilot-Project-Partnership ("Facedrive launches TraceSCAN Wearables pilot project in partnership with Labourers' International Union of North America (LiUNA)").

"Federal Court of Appeal to rule on the constitutionality of CASL", Nnovation LLP, December 23, 2019, online: https://nnovation.com/federal-court-of-appeal-to-rule-on-the-constitutionality-of-casl/ ("Federal Court of Appeal to rule on the constitutionality of CASL").

"Federal COVID-19 app launches after month-long delay", The Logic, July 31, 2020 ("Federal COVID-19 app launches after month-long delay").

"Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app", The Logic, June 4, 2020 ("Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app").

"Federal, Ontario governments launching apps to aid contact-tracing efforts", The Logic, June 18, 2020 ("Federal, Ontario governments launching apps to aid contact-tracing efforts").

"Federal, provincial watchdogs still waiting for full privacy assessment on national contact-tracing app", The Hill Times, June 29, 2020, online: https://mail.google.com/mail/u/0/#inbox/FMfcgxwJWXbpSPhMlPhFMFMqclHvwQzg?projector=1&messagePartId=0.1 ("Federal, provincial watchdogs still waiting for full privacy assessment on national contact-tracing app").

"Federally-backed COVID alert app now available in Ontario", July 31, 2020, CTV News, online: https://ottawa.ctvnews.ca/federally-backed-covid-alert-app-now-available-in-ontario-1.5046667 ("Federally-backed COVID alert app now available in Ontario").

"50 stats showing why companies need to prioritize consumer privacy", Forbes, June 22, 2020, online: https://www.forbes.com/sites/blakemorgan/2020/06/22/50-stats-showing-why-companies-need-to-prioritize-consumer-privacy/#11636bda37f6 ("50 stats showing why companies need to prioritize consumer privacy").

"Finding our way through privacy, data gaps and pandemic response", Canadian Lawyer (Chantal Bernier), May 19, 2020, online: https://www.canadianlawyermag.com/news/opinion/finding-our-way-through-privacy-data-gaps-and-pandemic-response/329733 ("Finding our way through privacy, data gaps and pandemic response").

"FIPA Joint Statement to PM Trudeau on Covid Shield" (note: re COVID Shield *Canada*), June 24, 2020, online: https://fipa.bc.ca/wordpress/wp-content/uploads/2020/06/20200624-Joint-Statement-on-Covid-Shield.pdf?utm_source=The+Logic+Master+List&utm_campaign=76e0ee2e18-Daily_Briefing_2020_June24_2&utm_medium=email&utm_term=0_325d5d3b52-76e0ee2e18-275653649 ("FIPA Joint Statement to PM Trudeau on Covid Shield") (note: joint statement by BC Freedom of Information and Privacy Association ["FIPA"], BC Civil Liberties Association ["BCLA"], Canadian Civil Liberties Association ["CCLA"], OpenMedia, CIPPIC, and International Civil Liberties Monitoring Group)

"Fitbit launches COVID-19 study; mindstrong raises $100M; Facedrive unveils TraceSCAN to stop COVID", Vator, May 29, 2020, online: https://vator.tv/news/2020-05-29-fitbit-launches-covid-19-study-mindspace-raises-100m-facedrive-unveils-tracescan-to-stop-covid-19 ("Facedrive unveils TraceSCAN to stop COVID").

"5 big EU countries blast Big Tech over approach to corona apps", Politico EU, May 26, 2020, online: https://www.politico.eu/article/5-eu-countries-blast-big-tech-over-corona-apps/?utm_source=The+Logic+Master+List&utm_campaign=1fdb9ae071-Daily_Briefing_2020_May26_2&utm_medium=email&utm_term=0_325d5d3b52-1fdb9ae071-275653649 ("5 big EU countries blast Big Tech over approach to corona apps").

"Five key provisions a federal privacy law should include", CPO Magazine, June 1, 2020, online: https://www.cpomagazine.com/data-protection/five-key-provisions-a-federal-privacy-law-should-include/ ("Five key provisions a federal privacy law should include").

"Ford urges people to download COVID-19 app as Ontario reports uptick in new cases", CBC News, July 31, 20202, online: https://www.cbc.ca/news/canada/toronto/covid-19-coronavirus-ontario-july-31-update-1.5670065 ("Ford urges people to download COVID-19 app as Ontario reports uptick in new cases").

"Four lessons: the digital health data", KPMG, November 2018, online: https://home.kpmg/xx/en/home/insights/2018/11/four-lessons-the-digital-health-data-race.html ("Four lessons: the digital health data").

"4 takeaways from contact tracing apps in other countries", CTV News, June 18, 2020, online: https://www.ctvnews.ca/health/coronavirus/4-takeaways-from-contact-tracing-apps-in-other-countries-1.4990497 ("4 takeaways from contact tracing apps in other countries").

"France: CNIL approves of implementation of StopCovid app", OneTrust DataGuidance, May 26, 2020, online: https://www.dataguidance.com/news/france-cnil-approves-implementation-stopcovid-app ("France: CNIL approves of implementation of StopCovid app").

"France anti-Covid-19 tracing app flop" (Google translation from French), Agence France-Presse, June 24, 2020 ("France anti-Covid-19 tracing app flop").

"France approves release of controversial COVID-19 tracking app", Euronews, May 28, 2020, online: https://www.euronews.com/2020/05/27/france-s-controversial-covid-19-tracking-phone-app-approved-by-lower-house-of-parliament ("France approves release of controversial COVID-19 tracking app").

"France backs virus tracing app following tough privacy debate", BNN Bloomberg, May 27, 2020, online: https://www.bnnbloomberg.ca/france-backs-virus-tracing-app-following-tough-privacy-debate-1.1441829 ("France backs virus tracing app following tough privacy debate").

"France offers a case study in the battle between privacy and coronavirus tracing apps", Venture Beat, May 18, 2020, online: https://venturebeat.com/2020/05/18/france-offers-a-case-study-in-the-battle-between-privacy-and-coronavirus-tracking-apps/ ("France offers a case study in the battle between privacy and coronavirus tracing apps").

"France's data protection watchdog reviews contact-tracing app StopCovid", TechCrunch, May 26, 2020, online: https://techcrunch.com/2020/05/26/frances-data-protection-watchdog-reviews-contact-tracing-app-stopcovid/ ("France's data protection watchdog reviews contact-tracing app StopCovid").

"French virus tracing app goes live amid debate over privacy", ABCnews.com, June 2, 2020, online: https://abcnews.go.com/Health/wireStory/french-virus-tracing-app-live-amid-debate-privacy-71016537 ("French virus tracing app goes live amid debate over privacy").

"Frequently asked questions about the Corona-Warn-App: what do the exposure check logs show?", Corona Warn-App Open Source Project, online: www.coronawarn.app/en/faq/#:~:text=The%20exposure%20check%20logs%20show,risk%20of%20infection%3F%20for%20details ("Frequently asked questions about the Corona-Warn-App: what do the exposure check logs show?").

G

"GDPR, a new privacy law, makes Europe world's leading tech watchdog", The New York Times, May 24, 2018, online: https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html ("GDPR, a new privacy law, makes Europe world's leading tech watchdog").

"Germany flips to Apple-Google approach on smartphone contact tracing", Reuters, April 26, 2020, online: https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J ("Germany flips to Apple-Google approach on smartphone contact tracing").

"Germany takes on Big Tech: inside the fight to curb the power of global data giants", The Globe and Mail, January 17, 2020, online: https://www.theglobeandmail.com/business/article-germany-takes-on-big-tech-inside-the-fight-to-curb-the-power-of/ ("Germany takes on Big Tech: inside the fight to curb the power of global data giants").

"Google API for exposure notification", Google, online: https://developers.google.com/android/exposure-notifications/exposure-notifications-api (accessed July 26, 2020) ("Google - Google API for exposure notification").

"Google, Apple struggle to regulate Covid-19 tracing apps", Wall Street Journal, June 5, 2020, online: https://www.wsj.com/articles/why-google-and-apple-stores-had-a-covid-19-app-with-ads-11591365499?utm_source=The+Logic+Master+List&utm_campaign=73d40ba05b-Daily_Briefing_2020_June5_2&utm_medium=email&utm_term=0_325d5d3b52-73d40ba05b-275653649 ("Google, Apple struggle to regulate Covid-19 tracing apps").

"Google COVID-19 exposure notifications service additional terms", Google, online: https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf (accessed July 26, 2020) ("Google API Terms of Service").

"Google exec outlines privacy measures in new contact-tracing API", The Wire Report, May 22, 2020 ("Google exec outlines privacy measures in new contact-tracing API").

"Google faces $5 billion lawsuit in US for tracking 'private' internet use", Reuters, June 2, 2020 ("Google faces $5 billion lawsuit in US for tracking 'private' Internet use").

"Google promises privacy with virus app but can still collect location", New York Times, Jul 20, 2020 ("Google promises privacy with virus app but can still collect location")

"Google sued for allegedly amassing user data, violating wiretap laws", The Logic, June 3, 2020 ("Google sued for allegedly amassing user data, violating wiretap laws").

"Government efforts to track virus through phone location data complicated by privacy concerns", Washington Post, March 19, 2020, online: https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/ ("Government efforts to track virus through phone location data complicated by privacy concerns").

"Group of Shopify volunteers create free COVID-19 contact tracing app", betakit.com, May 22, 2020, online: https://betakit.com/group-of-shopify-volunteers-create-free-covid-19-contact-tracing-app/ ("Group of Shopify volunteers create free COVID-19 contact tracing app").

H

"Hard questions for policy-makers about digital contact tracing", First Policy Response (Sean McDonald and Bianca Wylie, co-founders of Digital Public), May 21, 2020 ("Hard questions for policy-makers about digital contact tracing").

"Health ecommerce: serving and selling wellness in a jaded online world", Shopify: Industry Insights and Trends (Karine Bengualid), June 20, 2018, online: www.shopify.com/enterprise/heath-ecommerce-wellness-online ("Health ecommerce: serving and selling wellness in a jaded online world").

"Health Minister details pushback towards potential Canada-wide COVID-19 contact tracing app", Mobile Syrup, June 3, 2020, online: https://mobilesyrup.com/2020/06/03/health-minister-details-pushback-about-potential-canada-wide-covid-19-contact-tracing-app/ ("Health Minister details pushback towards potential Canada-wide COVID-19 contact tracing app").

"Healthcare: the great unlock", Andreesen Horowitz (Julie Yoo), August 7, 2020, online: https://a16z.com/2020/08/07/healthcare-technology-great-unlock/ ("Healthcare: the great unlock").

"HealthCare.gov breach exposes data of 75K individuals", Health Payer Intelligence, November 12, 2028, online: https://healthpayerintelligence.com/news/healthcare.gov-breach-exposes-data-of-75k-individuals ("HealthCare.gov breach exposes data of 75K individuals").

"HealthCare.gov breach exposed personal details of 75,000 including partial Social Security numbers", CNBC, November 9, 2018, online: https://www.cnbc.com/2018/11/09/healthcaregov-data-breach-exposed-personal-details-of-75000.html ("HealthCare.gov breach exposed personal details of 75,000 including partial Social Security numbers").

"Here's your daily COVID-19 roundup", The Logic, July 14, 2020 ("Here's your daily COVID-19 roundup, July 14, 2020").

"Hong Kong imposes strict COVID-19 measures, compulsory masks", CTV news, July 27, 2020, online: https://www.ctvnews.ca/health/coronavirus/hong-kong-imposes-strict-covid-19-measures-compulsory-masks-1.5040212 ("Hong Kong imposes strict COVID-19 measures, compulsory masks").

"Hospital 'overwhelmed' by cyberattacks fuelled by booming black market", CBC, June 2, 2020, online: https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422 ("Hospital 'overwhelmed' by cyberattacks fuelled by booming black market").

"Hospitals turn to big tech companies to store and analyze their data – leaving patients in the dark on privacy protections", Stat News, March 12, 2020, online: https://www.statnews.com/2020/03/12/hospitals-big-tech-store-analyze-data-privacy/ ("Hospitals turn to big tech companies to store and analyze their data – leaving patients in the dark on privacy protections").

"How do you trace Covid-19 while respecting privacy?" Anett Numan, speaker at 3-estonia briefing centre, April 2020, online: https://e-estonia.com/trace-covid-19-while-respecting-privacy/ ("How do you trace Covid-19 while respecting privacy?")

"How mobile phones could help trace the spread of COVID infections", The Record, June 1, 2020, online: https://www.therecord.com/ts/business/2020/06/01/how-mobile-phones-could-help-trace-the-spread-of-covid-infections.html ("How mobile phones could help trace the spread of COVID infections").

I

"If we must build a surveillance state, let's do it properly", Bloomberg, April 22, 2020, online: https://www.bloomberg.com/opinion/articles/2020-04-22/taiwan-offers-the-best-model-for-coronavirus-data-tracking ("If we must build a surveillance state, let's do it properly").

"Implementing privacy by design", David Krebs (Miller Thomson LLP), November 26, 2019, online: https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/implementing-privacy-by-design/ ("Implementing privacy by design").

"India is forcing people to use its Covid app, unlike any other democracy", MIT Technology Review, May 7, 2020, online: https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/ ("India is forcing people to use its Covid app, unlike any other democracy").

"Investigation: 'Without early warning you can't have early response': how Canada's world-class pandemic alert system failed", The Globe & Mail, July 25, 2020 (updated July 28) ("Without early warning you can't have early response").

"Ireland opens up its coronavirus contact tracing app for other governments to use", androidpolice.com, July 21, 2020 ("Ireland opens up its coronavirus contact tracing app for other governments to use").

"Is a successful contact tracing app possible? These countries think so", MIT Technology Review, August 10, 2020, online: https://www.technologyreview.com/2020/08/10/1006174/covid-contract-tracing-app-germany-ireland-success/ ("Is a successful contact tracing app possible? These countries think so").

"Is AWS liable in Capital One breach", Threat Post, October 25, 2019, online: https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/ ("Is AWS liable in Capital One breach").

"ISED 'digital charter' recommends enhancing OPC powers", The Wire Report, May 21, 2019 ("ISED 'digital charter' recommends enhancing OPC powers").

Israel limits coronavirus cellphone surveillance to 'special cases', reuters.com, May 24, 2020 ("Israel limits coronavirus cellphone surveillance to 'special cases'").

"Italy to launch Immuni contact-tracing app: here's what you need to know", The Local, June 5, 2020, online: https://www.thelocal.it/20200605/italy-to-begin-testing-immuni-contact-tracing-app-in-four-regions ("Italy to launch Immuni contact-tracing app: here's what you need to know").

"Italy's 'Immuni' COVID-19 contact tracing app uses Google, Apple tech: four regions will start piloting the exposure notification app starting next week", engadget, June 1, 2020, online: https://www.engadget.com/italy-coronavirus-contact-tracing-app-apple-google-covid-19-212811596.html ("Italy's 'Immuni' COVID-19 contact tracing app uses Google, Apple tech").

J

"Japan's contact-tracing method is old but gold", Asia Times, June 2, 2020, https://asiatimes.com/2020/06/japans-contact-tracing-method-is-old-but-gold/ ("Japan's contact-tracing method is old but gold").

"Japan releases contact-tracing app using Apple and Google tech (updated)", engadget, June 19, 2020, online: https://www.engadget.com/microsoft-built-japans-contacttracing-app-using-apple-and-google-tech-105556846.html ("Japan releases contact-tracing app using Apple and Google tech [updated]").

"Japan rolls out Microsoft- developed COVID-19 contact tracing app", The Verge, June 19, 2020, online: https://www.theverge.com/2020/6/19/21296603/japan-covid-19-contact-tracking-app-cocoa-released ("Japan rolls out Microsoft-developed COVID-19 contact tracing app").

"Japan's new virus contact-tracing app promises privacy in bid for reach", Japan Times, May 27, 2020 ("Japan's new virus contact-tracing app promises privacy in bid for reach").

"Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches", Financial Post, July 15, 2020 ("Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches").

"Joint statement on contact tracing", Global scientists and researchers, April 19, 2020, online: https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view ("Joint statement on contact tracing, global scientists and researchers").

K

N/A

L

"Lack of privacy oversight could hurt buy-in for COVID contact-tracing app, say critics", The Hill Times, July 2, 2020 ("Lack of privacy oversight could hurt buy-in for COVID contact-tracing app, say critics").

"Laughing UK health secretary launches COVID-19 test and trace programme with glitchy website and no phone app", The Register, May 28, 2020, online: https://www.theregister.co.uk/2020/05/28/england_covid19_contact_tracing_launch_shambles/ ("Laughing UK health secretary launches COVID-19 test and trace programme with glitchy website and no phone app").

"Law in the time of COVID-19, contact (tracing) high – part one", podcast (presented by McCarthy Tetrault LLP), June 3, 2020 ("Law in the time of COVID-19, contact (tracing) high – part one").

"Law in the time of COVID-19, contact (tracing) high – part two", podcast (presented by McCarthy Tetrault LLP), June 9, 2020 ("Law in the time of COVID-19, contact (tracing) high – part two").

"Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook", Orangeville.com, August 5, 2020, https://www.orangeville.com/news-story/10132037-less-than-4-of-canadians-have-the-covid-alert-tracing-app-despite-better-privacy-protection-than-facebook/ ("Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook")

"Lessons from the Italian COVID-19 contact tracing fiasco", ICLG, July 28, 2020, online: https://iclg.com/ibr/articles/14076-lessons-from-the-italian-covid-19-contact-tracing-fiasco-italy ("Lessons from the Italian COVID-19 contact tracing fiasco").

"Little enthusiasm among Quebec politicians as government mulls COVID-19 tracing app", CBC News, August 13, 2020, online: https://www.cbc.ca/news/canada/montreal/quebec-covid-19-contact-tracing-app-1.5683914 ("Little enthusiasm among Quebec politicians as government mulls COVID-19 tracing app").

"Logic Briefing: Northern exposure notification", The Logic, June 18, 2020 ("Logic Briefing: Northern exposure notification").

M

"Majority of Americans say they won't use COVID contact tracing apps", Avira, June 2020, online: https://www.avira.com/en/covid-contact-tracing-app report ("Majority of Americans say they won't use COVID contact tracing apps").

"Majority of Canadians do not approve of a mandatory contact tracing app: Mainstreet poll", iPolitics, May 12, 2020 ("Majority of Canadians do not approve of a mandatory contact tracing app: Mainstreet poll").

"Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says", July 24, 2020, Global News, online: https://globalnews.ca/news/7213653/coronavirus-app-user-friendly-delay-hajdu/# ("Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says").

"Microsoft leaves 250M customer service records open to the Web", Threat Post, January 22, 2020, online: https://threatpost.com/microsoft-250m-customer-service-records-open/152086/ ("Microsoft leaves 250M customer service records open to the Web").

Mimik Technology Inc. website, mimik.com (accessed June 1, 2020) ("Mimik website").

"Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app", CBC News, August 13, 2020, online: https://www.cbc.ca/news/technology/covid-19-alert-app-myths-privacy-1.5684089 ("Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app").

"Mobile contact-tracing app can help Alberta slow spread of COVID-19, top doctor says", CBC, May 1, 2020, online: https://www.cbc.ca/news/canada/edmonton/deena-hinshaw-abtracetogether-covid-19-coronavirus-1.5552413 ("Mobile contact-tracing app can help Alberta slow spread of COVID-19, top doctor says").

"More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive", Colin Bennett blog, May 19, 2020 ("More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive").

"Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic", The Washington Post, April 29, 2020, online: https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/ ("Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic").

N

"New Brunswick: new rules for collecting contact tracing info coming amid privacy concerns", CBC.ca News, July 16, 2020 ("New Brunswick: New rules for collecting contact tracing info coming amid privacy concerns").

"New Brunswick's plan for COVID-19 contact tracing pp thwarted by federal government", Mobile Syrup, June 21, 2020, online: https://mobilesyrup.com/2020/06/21/new-brunswicks-covid-19-contact-tracing-app-thwarted-federal-government/ ("New Brunswick's plan for COVID-19 contact tracing pp thwarted by federal government").

"New COVID-19 notification app rolls out in Ontario", CBC News, July 31, 2020, online: https://www.cbc.ca/news/politics/covid-pandemic-app-ontario-1.5670239 ("New COVID-19 notification app rolls out in Ontario").

"New mobile app meant to help track COVID-19 in Ontario delayed", CTV News, July 2, 2020, online: https://toronto.ctvnews.ca/new-mobile-app-meant-to-help-track-covid-19-in-ontario-delayed-1.5007761 ("New mobile app meant to help track COVID-19 in Ontario delayed").

"New Zealand's COVID-19 Tracer app won't help open a 'travel bubble' with Australia anytime soon", The Conversation, May 20, 2020, online: https://theconversation.com/new-zealands-covid-19-tracer-app-wont-help-open-a-travel-bubble-with-australia-anytime-soon-139026 ("New Zealand's COVID-19 Tracer app won't help open a 'travel bubble' with Australia anytime soon").

"NHS contact tracing app isn't really anonymous, is riddled with bugs, and is open to abuse. Good thing we're not in the middle of a pandemic, eh?", The Register, May 14, 2020, online: https://www.theregister.co.uk/2020/05/14/nhs_contact_tracing_app/ ("NHS contact tracing app isn't really anonymous, is riddled with bugs, and is open to abuse. Good thing we're not in the middle of a pandemic, eh?")

"No, coronavirus apps don't need 60% adoption to be effective", MIT Technology Review, June 5, 2020, online: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/?utm_source=The+Logic +Master+List&utm_campaign=73d40ba05b-Daily_Briefing_2020_June5_2&utm_medium=email&utm_term=0_325d5d3b52-73d40ba05b-275653649 ("No, coronavirus apps don't need 60% adoption to be effective").

"No longer fit for purpose: why Canadian privacy law needs an update", Michael Geist blog, March 6, 2018, online: http://www.michaelgeist.ca/2018/03/no-longer-fit-purpose-canadian-privacy-law-needs-update/ ("No longer fit for purpose: why Canadian privacy law needs an update").

"North Dakota's COVID-19 app has been sending data to Foursquare and Google", Fast Company, May 20, 2020 ("North Dakota's COVID-19 app has been sending data to Foursquare and Google").

"Northern Ireland launches UKs first Covid-19 contact-tracing app", Digital Health, on or around Aug 5, 2020, https://www.digitalhealth.net/2020/08/northern-ireland-launches-uks-first-covid-19-contact-tracing-app/ ("Northern Ireland launches UKs first Covid-19 contact-tracing app").

"Norway pulls its coronavirus contacts-tracing app after privacy watchdog's warning", Tech Crunch, June 15, 2020, online: https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/?utm_source=The+ Logic+Master+List&utm_campaign=54c2d2cd00-Daily_Briefing_2020_June15_2&utm_medium=email&utm_term=0_325d5d3b52-54c2d2cd00-275653649 ("Norway pulls its coronavirus contacts-tracing app after privacy watchdog's warning").

"Notification: apps won't contain the outbreak of COVID-19", CIGI (Sean McDonald and Bianca Wylie), June 25, 2020, online: https://www.cigionline.org/articles/notification-apps-wont-contain-outbreak-covid-19 ("Notification: apps won't contain the outbreak of COVID-19").

O

"OECD policy responses to coronavirus (COVID-19): cities policy response", OECD, July 23, 2020, online: http://www.oecd.org/coronavirus/policy-responses/cities-policy-responses-fd1053ff/ ("OECD policy responses to coronavirus [COVID-19]: cities policy response").

"One app per province? How Canada's federalism complicates contact tracing", Heinrich Boll Stiftung (Teresa Scassa), May 13, 2020, online: https://us.boell.org/en/2020/05/13/one-app-province-how-canadas-federalism-complicates-digital-contact-tracing ("One app per province? How Canada's federalism complicates contact tracing").

"1 million downloads in 5 weeks - the tech company fighting COVID in Canada", Stockhouse.com, Aug 5, 2020, https://stockhouse.com/news/press-releases/2020/08/05/1-million-downloads-in-5-weeks-the-tech-company-fighting-covid-in-canada ("1 million downloads in 5 weeks - the tech company fighting COVID in Canada").

"One of the first contact tracing apps violates its own privacy policy", The Washington Post, May 21, 2020 ("One of the first contact tracing apps violates its own privacy policy").

"Only 29 percent of Canadians are 'very likely' to download COVID Alert app: survey 41 percent of respondents said privacy concerns were the biggest reason holding them back from downloading the app", Mobile Syrup, July 24, 2020 ("Only 29 percent of Canadians are 'very likely' to download COVID Alert app").

"Ontario considers privacy overhaul", The Wire Report, August 14, 2020 ("Ontario considers privacy overhaul").

"Ontario's construction industry pushes for wearable COVID-19 tracing app", Globe & Mail, August 4, 2020 ("Ontario's construction industry pushes for wearable COVID-19 tracing app").

"Ontario Government agrees to human rights groups' demands to end police access to COVID database", CCLA, August 17, 2020, online: https://ccla.org/covid-police-data/?utm_source=The+Logic+Master+List&utm_campaign=25ece2a9a6-Daily_Briefing_2020_August17_1&utm_medium=email&utm_term=0_325d5d3b52-25ece2a9a6-275653649 ("Ontario Government agrees to human rights groups' demands to end police access to COVID database").

"Ontario launches consultation on new private sector data protection law", Teresa Scassa's blog, August 13, 2020, online: http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=329:ontario-launches-consultation-on-a-new-private-sector-data-protection-law&Itemid=80 ("Ontario launches consultation on new private sector data protection law").

"Ontario Privacy Laws for Lawyers", McCague Borlack LLP, January 2014, online: https://mccagueborlack.com/emails/articles/ht-privacy-lawyers.html ("Ontario Privacy Laws for Lawyers").

"Ontario recognizes new privacy tort", Torys LLP, January 29, 2020, online: https://www.torys.com/insights/publications/2020/01/ontario-recognizes-new-privacy-tort ("Ontario recognizes new privacy tort").

"OPC issues guidance on federal privacy laws in light of the COVID-19 outbreak", Deeth Williams Wall, April 9, 2020, online: https://www.dww.com/articles/opc-issues-guidance-on-federal-privacy-laws-light-of-covid19-outbreak ("OPC issues guidance on federal privacy laws in light of the COVID-19 outbreak").

"OPC releases mandatory breach reporting guidance", Miller Thomson, November 1, 2018, online: https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/opc-releases-mandatory-breach-reporting-guidance/ ("OPC releases mandatory breach reporting guidance").

"OPH contact tracing tech on hold while province and feds develop their own", Ottawa Citizen, May 22, 2020, online: https://ottawacitizen.com/news/local-news/oph-contact-tracing-tech-on-hold-while-province-and-feds-develop-their-own ("OPH contact tracing tech on hold while province and feds develop their own").

"Opposition parties say COVID-19 tracing app is a non-starter", Montreal Gazette, August 14, 2020, online: https://montrealgazette.com/news/quebec/opposition-parties-says-covid-19-tracing-app-is-a-non-starter ("Opposition parties say COVID-19 tracing app is a non-starter").

"Ottawa-based Shopify volunteers to launch COVID-19 exposure notification solution", Mobile Syrup, May 28, 2020, online: https://mobilesyrup.com/2020/05/28/ottawa-based-shopify-volunteers-launch-covid-19-exposure-notification-solution/ ("Ottawa-based Shopify volunteers to launch COVID-19 exposure notification solution").

"Ottawa plans up to $10 million for COVID Alert public awareness campaign", The Logic (Interview with Minister Murray), August 7, 2020 ("Ottawa plans up to $10 million for COVID Alert public awareness campaign").

"Ottawa promotes contact tracing app for Canadians in fight against the spread of COVID-19", Globe & Mail, June 18, 2020 ("Ottawa promotes contact tracing app for Canadians in fight against the spread of COVID-19").

"Ottawa ready to help co-ordinate provincial testing, contact tracing: Trudeau", Red Deer Advocate, May 15, 2020 ("Ottawa ready to help co-ordinate provincial testing, contact tracing: Trudeau").

"Ottawa rolls out its own contact tracing app, raising questions about ABTraceTogether", Calgary Herald, August 1, 2020, online: https://calgaryherald.com/news/local-news/alberta-says-feds-blocking-update-to-abtracetogether-app ("Ottawa rolls out its own contact tracing app, raising questions about ABTraceTogether").

"Our health is all we have. But now Google wants it too", The Guardian, August 2, 2020, online: https://www.theguardian.com/business/2020/aug/01/health-data-google-wants-it-all-fitbit-deal-big-tech ("Our health is all we have. But now Google wants it too").

"Outdated privacy laws may hamper COVID-19 tracing: Therrien", The Wire Report, May 29, 2020 ("Outdated privacy laws may hamper COVID-19 tracing: Therrien").

P

"Palantir's NHS data project 'may outlive coronavirus crisis'", NS Tech, April 30, 2020, online: https://tech.newstatesman.com/coronavirus/palantir-covid19-datastore-coronavirus ("Palantir's NHS data project 'may outlive coronavirus crisis'").

"Pandemic has increased the need for privacy rights, OPC told Guilbeault", The Wire Report, June 30, 2020 ("Pandemic has increased the need for privacy rights, OPC told Guilbeault").

"Pandimik-FAQ", https://mimik.com/pandimik/ (accessed June 1, 2020) ("Pandimik FAQ").

"P.E.I. to see how COVID-19 app fares in Ontario before final decision on use", Atlantic CTV News, August 4, 2020 ("P.E.I. to see how COVID-19 app fares in Ontario before final decision on use").

"Personal data of more than 144K Canadians breached by federal government", Infosecurity Magazine, February 17, 2020, online: https://www.infosecurity-magazine.com/news/personal-data-of-144k-canadians/ ("Personal data of more than 144K Canadians breached by federal government").

"PIAC wants the CRTC to investigate pandemic contact-tracing apps", cartt.ca, May 5, 2020 ("PIAC wants the CRTC to investigate pandemic contact-tracing apps").

"Plans for single COVID-19 contract tracing app facing resistance: health minister", CTVnews.ca, June 1, 2020, online: https://www.ctvnews.ca/politics/plans-for-single-covid-19-contact-tracing-app-facing-resistance-health-minister-1.4963895 ("Plans for single COVID-19 contract tracing app facing resistance: health minister").

"PM says a national contact tracing app is coming next month, how will it work?", CTV News, June 18, 2020, online: https://www.ctvnews.ca/health/coronavirus/pm-says-a-national-contact-tracing-app-is-coming-next-month-how-will-it-work-1.4989702 ("PM says a national contact tracing app is coming next month, how will it work?").

"Poland rolls out privacy-secure coronavirus tracking app", Reuters, June 9, 2020, online: https://www.reuters.com/article/us-health-coronavirus-poland-tech/poland-rolls-out-privacy-secure-coronavirus-tracking-app-idUSKBN23G208?utm_source=The+Logic+Master+List&utm_campaign= 777c4566c3-Daily_Briefing_2020_June9_2&utm_medium=email&utm_term=0_325d5d3b52-777c4566c3-275653649 ("Poland rolls out privacy-secure coronavirus tracking app").

"Poland switches to privacy-conscious contact tracing", E&T, June 9, 2020, online: https://eandt.theiet.org/content/articles/2020/06/poland-switches-to-privacy-conscious-contact-tracing-app/ ("Poland switches to privacy-conscious contact tracing").

"Potential privacy threat to Android owners using COVID exposure notification app won't be fixed until 'later in the third quarter'", The Hill Times, July 31, 2020 ("Potential privacy threat to Android owners using COVID exposure notification app won't be fixed until 'later in the third quarter'")

"Privacy 101, for people who are new to privacy", Salinger Privacy, May 3, 2019, online: https://www.salingerprivacy.com.au/2019/05/03/privacy-101/ ("Privacy 101, for people who are new to privacy").

"Privacy and COVID-19 mini-summit", hosted by Canadian Anonymization Network ("CANON"), Presenter Pollyanna Sanderson, Policy Counsel, Future of Privacy Forum, June 17, 2020 ("Privacy and COVID-19 mini-summit").

"Privacy and security are key to contact tracing apps", Financial Post (Blackberry Chief Technology Officer Charles Eagan), July 17, 2020 ("Privacy and security are key to contact tracing apps").

"Privacy commissioners: privacy laws not a barrier to effective COVID-19 response, emphasize compliance when using contact tracing apps", Miller Thomson, May 12, 2020, online: https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/privacy-commissioners-privacy-laws-not-a-barrier-to-effective-covid-19-response-emphasize-compliance-when-using-contact-tracing-apps/ ("Privacy commissioners: privacy laws not a barrier to effective COVID-19 response, emphasize compliance when using contact tracing apps").

"Privacy expert says flawed Alberta COVID-19 contact tracking app shouldn't have been released", IT World Canada, May 4, 2020, online: https://www.itworldcanada.com/article/privacy-expert-says-flawed-alberta-covid-19-contact-tracking-app-shouldnt-have-been-released/430252 ("Privacy expert says flawed Alberta COVID-19 contact tracking app shouldn't have been released").

"Privacy experts concerned about next stage of Ontario's reopening plan", Kitchener Today, June 11, 2020, online: https://www.kitchenertoday.com/coronavirus-covid-19-local-news/privacy-experts-concerned-about-next-stage-of-ontarios-reopening-plan-2426690 ("Privacy experts concerned about next stage of Ontario's reopening plan").

"Privacy experts support call for national plan for COVID-19 contact tracing app", IT World Canada, May 5, 2020, online: https://www.itworldcanada.com/article/privacy-experts-support-call-for-national-plan-for-covid-contact-tracing-app/430296 ("Privacy experts support call for national plan for COVID-19 contact tracing app").

"Privacy fears threaten New York City's coronavirus tracing efforts", Politico, June 4, 2020, online: https://www.politico.com/states/new-york/albany/story/2020/06/04/privacy-fears-threaten-new-york-citys-coronavirus-tracing-efforts-1290657 ("Privacy fears threaten New York City's coronavirus tracing efforts").

"Privacy in a pandemic: privacy laws matter", Gowling WLG, April 15, 2020, online: https://gowlingwlg.com/en/insights-resources/articles/2020/privacy-in-a-pandemic-privacy-laws-matter/ ("Privacy in a pandemic: privacy laws matter").

"Privacy in a post-pandemic world", Forbes, June 23, 2020, online: https://www.forbes.com/sites/forbestechcouncil/2020/06/23/privacy-in-a-post-pandemic-world/#3ac93dab2b0a ("Privacy in a post-pandemic world").

Privacy International, online: https://privacyinternational.org

"Privacy in the age of COVID-19", Circle ID (Doug Dawson, President, CCG Consulting), June 3, 2020, online: http://www.circleid.com/posts/20200603-privacy-in-the-age-of-covid-19/ ("Privacy in the age of COVID-19").

"Privacy in the age of COVID: an IDAC investigation of COVID-19 apps", International Digital Accountability Council ("IDAC"), June 5, 2020, online: https://digitalwatchdog.org/privacy-in-the-age-of-covid-an-idac-investigation-of-covid-19-apps/ ("Privacy in the age of COVID: an IDAC investigation of COVID-19 apps") and accompanying report with the same title, online: https://digitalwatchdog.org/wp-content/uploads/2020/06/IDAC-COVID19-Mobile-Apps-Investigation.pdf ("IDAC report on privacy and COVID-19 apps").

"Privacy in the balance", CBA National Magazine, April 15, 2020, online: https://www.nationalmagazine.ca/en-ca/articles/law/in-depth/2020/privacy-in-the-balance ("Privacy in the balance").

"Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy", *Phil. Trans. R. Soc*. A 374: 20160118, http://dx.doi.org/10.1098/rsta.2016.0118, accepted: 3 October 2016, online: https://www.law.berkeley.edu/wp-content/uploads/2017/07/Privacy-is-an-essentially.pdf ("Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy").

"Privacy is not the problem with the Apple-Google contact-tracing toolkit", The Guardian (Michael Veale, co-developer of DP-3T and lecturer in digital rights and regulation in the faculty of laws, University College London), July 1, 2020, online:

https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights ("Privacy is not the problem with the Apple-Google contact-tracing toolkit").

"Privacy officials say LifeLabs has asked court to limit their breach report", Globe & Mail, July 29, 2020 ("Privacy officials say LifeLabs has asked court to limit their breach report").

"Privacy Penalties – Canadian Competition Bureau wades into privacy enforcement", ICLG.com (McMillan LLP), May 28, 2020 ("Privacy Penalties – Canadian Competition Bureau wades into privacy enforcement").

"Privacy, security concerns as India forces virus-tracing app on millions", CBS News, May 27, 2020, online: https://www.cbsnews.com/news/coronavirus-india-contact-tracing-app-privacy-data-security-concerns-aarogya-setu-forced-on-millions/ ("Privacy, security concerns as India forces virus-tracing app on millions").

"Privacy watchdogs taking a look at Tim Hortons app's location tracking technology", Financial Post, June 18, 2020, online: https://business.financialpost.com/technology/privacy-watchdogs-taking-a-look-at-tim-hortons-apps-location-tracking-technology?utm_medium=Social&utm_source=Twitter#Echobox=1592490848 ("Privacy watchdogs taking a look at Tim Hortons app's location tracking technology").

"Protect our privacy during COVID-19", OpenMedia, online: https://action.openmedia.org/page/59978/petition/1?locale=en-US ("OpenMedia CTA petition").

"Provide advance notice to the Google Play App Review team", Google, online: https://support.google.com/googleplay/android-developer/contact/adv_note (accessed July 26, 2020) ("Google - Provide advance notice to the Google Play App Review team").

"Province hoping Albertans will download COVID-19 app called AB Trace Together", Todayville, around May 1, 2020, online: https://www.todayville.com/province-hoping-albertans-will-download-covid-19-app-called-ab-trace-together/ ("Province hoping Albertans will download COVID-19 app called AB Trace Together").

"Province's plan for COVID-19 contact-tracing app denied by Ottawa", CBC, June 19, 2020, online: https://www.cbc.ca/news/canada/new-brunswick/covid-19-contact-tracing-app-new-brunswick-national-1.5618973 ("Province's plan for COVID-19 contact-tracing app denied by Ottawa").

Q

"Quality issues may be the stumbling block in the race for contact tracing apps", Stat News, July 28, 2020, online: https://www.statnews.com/2020/07/28/quality-issues-stumbling-block-contact-tracing-apps/ ("Quality issues may be the stumbling block in the race for contact tracing apps").

"Quebec: Bill seeking data protection reform introduced to National Assembly", OneTrust DataGuidance, June 12, 2020, online: https://www.dataguidance.com/news/quebec-bill-seeking-data-protection-reform-introduced-national-assembly ("Quebec: Bill seeking data protection reform introduced to National Assembly").

"Quebec Assembly signals possible split from COVID Alert system", iPolitics, August 14, 2020, online: https://ipolitics.ca/2020/08/14/quebec-assembly-signals-possible-split-from-covid-alert-system/ ("Quebec Assembly signals possible split from COVID Alert system").

"Quebec launches online consultation for COVID-19 contact tracing app", CTV News Montreal, July 8, 2020, online: https://montreal.ctvnews.ca/quebec-launches-online-consultation-for-covid-19-contact-tracing-app-1.5015900 ("Quebec launches online consultation for COVID-19 contact tracing app").

"Quebec turns to public to determine demand for a COVID-19 tracing app", Montreal Gazette, July 8, 2020, online: https://montrealgazette.com/news/local-news/quebec-turns-to-public-to-determine-demand-for-a-covid-19-tracing-app ("Quebec turns to public to determine demand for a COVID-19 tracing app")

R

"Race to trace: security and privacy of COVID-19 contact tracing apps", Report, Cybersecure Policy Exchange ("CPE"), Ryerson University, June 8, 2020, online: https://www.cybersecurepolicy.ca/racetotrace ("CPE Race to trace: security and privacy of COVID-19 contact tracing apps").

"Report finds massive drop in Canadians' willingness to disclose personal information for free online services", Canadian Internet Registration Authority (CIRA), May 28, 2020 ("Report finds massive drop in Canadians' willingness to disclose personal information for free online services").

"Republican senators to introduce the COVID-19 Consumer Data Protection Act", May 1, 2020, iapp.org ("Republican senators to introduce the COVID-19 Consumer Data Protection Act").

"Requirement for N.B. restaurants to collect contact information raises privacy questions", Global News, July 12, 2020 ("Requirement for N.B. restaurants to collect contact information raises privacy questions").

"Ryerson cyber-policy group calls for law preventing employers and businesses making contact-tracing app mandatory", The Logic, June 8, 2020 ("Ryerson cyber-policy group calls for law preventing employers and businesses making contact-tracing app mandatory").

S

"Saudi Arabia releases contact tracing app", Digital Watch Observatory, June 14, 2020, online: https://dig.watch/updates/saudi-arabia-releases-contact-tracing-app ("Saudi Arabia releases contact tracing app").

"'Shoe-leather' contact tracing works", Pluralistic (Cory Doctorow), May 19, 2020 ("'Shoe-leather' contact tracing works").

"Shopify, Blackberry, and Ontario to help Canada launch contact tracing app", IT World Canada, June 18, 2020, online: https://www.itworldcanada.com/article/shopify-blackberry-and-ontario-to-help-canada-launch-contact-tracing-app/432236 ("Shopify, Blackberry, and Ontario to help Canada launch contact tracing app").

"Shopify POS review", Merchant Maverick (Matt Sherman), May 6, 2020, online: www.merchantmaverick.com/reviews/shopify-pos-review/ ("Shopify POS review").

"Shopify Volunteers Release Open-Sourced Contact-Tracing App", Born Digital, May 25, 2020, online: https://www.borndigital.com/2020/05/25/shopify-volunteers-release-open-sourced-contact-tracing-app ("Shopify volunteers release open-sourced contact-tracing app").

"Shrems II: the saga continues", McCarthy Tetrault LLP, July 16, 2020, online: https://www.mccarthy.ca/en/insights/blogs/techlex/schrems-ii-saga-continues ("Shrems II: the saga continues").

"Snap has a new partnership that opens it up to hundreds of thousands of advertisers", yahoo!finance (Megan Graham), April 29, 2019, online: finance.yahoo.com/news/snap-partnership-opens-hundreds-thousands-120008494.html ("Snap has a new partnership that opens it up to hundreds of thousands of advertisers").

"Staff is not the Commission, says PIAC", cartt.ca**,** May 14, 2020 ("Staff is not the Commission, says PIAC").

"Supreme Court of Canada decision raises interesting issues about jurisdiction over privacy-impactful technologies", Teresa Scassa blog, July 15, 2020 ("Supreme Court of Canada decision raises interesting issues about jurisdiction over privacy-impactful technologies").

"Surveillance giants: how the business model of Google and Facebook threatens human rights", Amnesty International, November 21, 2019, online: https://www.amnesty.org/en/documents/pol30/1404/2019/en/ ("Surveillance Giants: how the business model of Google and Facebook threatens human rights").

"Surveys show conflicting support by Canadians for COVID-19 tracing app", itworldcanada.ca, May 14th, 2020 ("Surveys show conflicting support by Canadians for COVID-19 tracing app").

"Switzerland launches SwissCovid tracing app for residents", Swiss Info Science ("SWI"), June 25, 2020, online: https://www.swissinfo.ch/eng/switzerland-launches-swisscovid-contact-tracing-app-for-residents/45859778 ("Switzerland launches SwissCovid tracing app for residents").

T

"Take part in our research: Do you want to slow the spread of COVID-19?", Canadian Digital Service (Beta version of COVID Shield Canada), online: https://digital.canada.ca/covid-app-beta/ (accessed July 22, 2020) ("CDS – Take part in our research: Do you want to slow the spread of COVID-19?").

"TCN Coalition applauds Apple and Google's digital contact tracing announcement", TCN Coalition, April 10, 2020, online: https://drive.google.com/file/d/ 1Sl6- afmJ1OFiQlC RjtLBXv1g -OllY/view ("TCN Coalition applauds Apple and Google's digital contact tracing announcement").

"Tech's first big plan to tackle Covid-19 stumbles: 'an app is not going to fix this'", Wall Street Journal, May 29, 2020 ("Tech's first big plan to tackle Covid-19 stumbles: 'an app is not going to fix this'").

"Technology Theatre", CIGI (S. McDonald), July 13, 2020, online: https://www.cigionline.org/articles/technology-theatre ("Technology Theatre").

"Telecom in the spotlight in new Bains mandate letter", The Wire Report, December 13, 2019 ("Telecom in the spotlight in new Bains mandate letter").

"TELUS Data for Good program to provide de-identified network mobility data and insights to the Natural Sciences and Engineering Research Council of Canada in support of COVID-19 research", Telus News Release, May 20, 2020, online: https://www.globenewswire.com/news-release/2020/05/20/2036577/0/en/TELUS-Data-for-Good-program-to-provide-de-identified-network-mobility-data-and-insights-to-the-Natural-Sciences-and-Engineering-Research-Council-of-Canada-in-support-of-COVID-19-re.html ("TELUS Data for Good program to provide de-identified network mobility data and insights to the Natural Sciences and Engineering Research Council of Canada in support of COVID-19 research").

"Telus to provide data from networks to Ottawa to help combat spread of COVID-19", Globe & Mail, May 20, 2020 ("Telus to provide data from networks to Ottawa to help combat spread of COVID-19").

"Telus to provide network mobility data and insights in support of Covid-19 research", cartt.ca, May 20, 2020 ("Telus to provide network mobility data and insights in support of Covid-19 research").

"Telus to share aggregate location data with government researchers", The Wire Report, May 20, 2020 ("Telus to share aggregate location data with government researchers").

"Testing the public's trust: Quebec premier mulls adopting contact-tracing app", CBC news, May 19, 2020, online: https://www.cbc.ca/news/canada/montreal/quebec-premier-considers-covi-contact-tracing-app-1.5576122 ("Testing the public's trust: Quebec premier mulls adopting contact-tracing app").

"The case against lockdowns: can we fight the COVID-19 outbreak without confining people to their homes?", National Post, May 1, 2020 ("The case against lockdowns: can we fight the COVID-19 outbreak without confining people to their homes?").

"The case for contact tracing apps build on Apple and Google's exposure notification system", techdirt.com, May 20, 2020, online: https://www.techdirt.com/articles/20200520/10571644539/case-contact-tracing-apps-built-apple-googles-exposure-notification-system.shtml ("The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System")

"The invisible selling machine", Magzter (Stephen M. Baldwin), March 15, 2017, online: www.magzter.com/article/Business/Fortune/The-Invisible-Selling-Machine ("The invisible selling machine").

The Logic:

- May 26, 2020 ("The Logic, May 26, 2020").
- July 30, 2020 ("The Logic, July 30, 2020")
- August 4, 2020 ("The Logic, August 4, 2020")
- August 10, 2020 ("The Logic, August 10, 2020")

"The privacy, data protection and cybersecurity law review - edition 6: Canada", The Law Reviews (Shaun Brown, nNovation LLP), October 2019, online: https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210002/canada ("The privacy, data protection and cybersecurity law review - edition 6: Canada").

"The privacy pragmatic as privacy vulnerable", Urban J.M. and Hoofnagle C.J. (Berkeley Law), Symposium on Usable Privacy and Security, 2014, online: https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s1p2.pdf ("The privacy pragmatic as privacy vulnerable").

"The rise of the digital robber barons: is government up to the task at hand?", Rob Normey, July 2, 2020 ("The rise of the digital robber barons").

"The State of Rhode Island is a trailblazer in testing and contact tracing efforts", Salesforce, Customer Success Stories, online: https://www.salesforce.com/customer-success-stories/state-of-rhode-island/ (accessed July 30, 2020) ("Salesforce – The State of Rhode Island is a trailblazer in testing and contact tracing efforts").

"The tech 'solutions' for coronavirus take the surveillance state to the next level", The Guardian (Opinion - Evgeny Morozov), April 15, 2020, online: https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt ("The tech 'solutions' for coronavirus take the surveillance state to the next level"). (note: Evgeny Morozov is author of "Net Delusion: The Dark Side of Internet Freedom", visiting scholar at Stanford University, and Schwartz fellow at New America Foundation)

"The US's draft law on contact tracing apps is a step behind Apple and Google", MIT Technology Review, June 2, 2020, online: https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/ ("The US's draft law on contact tracing apps is a step behind Apple and Google").

"The world's first contact-tracing app using Google and Apple's API goes live", ZDnet.com, May 28, 2020, online: https://www.zdnet.com/article/the-worlds-first-contact-tracing-app-using-google-and-apples-api-goes-live/ ("The world's first contact-tracing app using Google and Apple's API goes live").

"Thinking through the manifold ramifications of collecting smartphone data for contact tracing", The Daring Fireball (John Gruber), May 18, 2020, online: https://daringfireball.net/linked/2020/05/18/healy-privacy-exposure-notification ("Thinking through the manifold ramifications of collecting smartphone data for contact tracing").

"Tim Hortons facing class-action lawsuit over app location tracking", Financial Post, June 30, 2020, online: https://business.financialpost.com/technology/tim-hortons-facing-class-action-lawsuit-over-app-location-tracking?utm_medium=Social&utm_source=Twitter#Echobox=1593546731 ("Tim Hortons facing class-action lawsuit over app location tracking").

"Tim Hortons scaling back data collection as four privacy watchdogs announce joint investigation into app", Financial Post, June 29, 2020, online: https://business.financialpost.com/technology/four-privacy-commissioners-launch-joint-investigation-of-tim-hortons-app ("Tim Hortons scaling back data collection as four privacy watchdogs announce joint investigation into app").

"TLDR; 15 Excerpts from the Privacy Commissioner's Review of Health Canada's COVID 19 Contact Tracing App", Claudiu Popa, August 1, 2020 ("TLDR; 15 Excerpts from the Privacy Commissioner's Review of Health Canada's COVID 19 Contact Tracing App").

"To protect our privacy rights, COVID-19 surveillance measures need a squeaky wheel", The Hill Times (Adam Gordon), June 15, 2020 ("To protect our privacy rights, COVID-19 surveillance measures need a squeaky wheel").

"Toronto's contact tracing system struggles to get up to speed", Toronto Star, May 31, 2020, online: https://www.thestar.com/opinion/2020/05/31 /battling-fast-moving-covid-19-torontos-contact-tracing-system-struggles-to-get-up-to-speed.html ("Toronto's contact tracing system struggles to get up to speed").

TraceSCAN website, www.TraceScan.ca (accessed June 1, 2020) ("TraceSCAN website").

"Trace me on my cellphone", The Logic:

- "Trace me on my cellphone", The Logic, July 22, 2020 ("Trace me on my cellphone, July 22, 2020")
- "Trace me on my cellphone", The Logic, July 6, 2020 ("Trace me on my cellphone, July 6, 2020")
- "Trace me on my cellphone", The Logic, June 29, 2020 ("Trace me on my cellphone, June 29, 2020")
- "Trace me on my cellphone", The Logic, June 23, 2020 ("Trace me on my cellphone, June 23, 2020")
- "Trace me on my cellphone", The Logic, June 19, 2020 ("Trace me on my cellphone, June 19, 2020")
- "Trace me on my cellphone", The Logic, June 16, 2020 ("Trace me on my cellphone, June 16, 2020")

- "Trace me on my cellphone", The Logic, June 15, 2020 ("Trace me on my cellphone, June 15, 2020")
- "Trace me on my cellphone", The Logic, June 12, 2020 ("Trace me on my cellphone, June 12, 2020")
- "Trace me on my cellphone", The Logic, June 10, 2020 ("Trace me on my cellphone, June 10, 2020")
- "Trace me on my cellphone", The Logic, June 9, 2020 ("Trace me on my cellphone, June 9, 2020")
- "Trace me on my cellphone", The Logic, June 5, 2020 ("Trace me on my cellphone, June 5, 2020")
- "Trace me on my cellphone", The Logic, June 4, 2020 ("Trace me on my cellphone, June 4, 2020")
- "Trace me on my cellphone", The Logic, May 29, 2020 ("Trace me on my cellphone, May 29, 2020")
- "Trace me on my cellphone", The Logic, May 28, 2020 ("Trace me on my cellphone, May 28, 2020")
- "Trace me on my cellphone", The Logic, May 27, 2020 ("Trace me on my cellphone, May 27, 2020")
- "Trace me on my cellphone", The Logic, May 26, 2020 ("Trace me on my cellphone, May 26, 2020")
- "Trace me on my cellphone", The Logic, May 25, 2020 ("Trace me on my cellphone, May 25, 2020")
- "Trace me on my cellphone", The Logic, May 22, 2020 ("Trace me on my cellphone, May 22, 2020")
- "Trace me on my cellphone", The Logic, May 21, 2020 ("Trace me on my cellphone, May 21, 2020")
- "Trace me on my cellphone", The Logic, May 20, 2020 ("Trace me on my cellphone, May 20, 2020")
- "Trace me on my cellphone", The Logic, May 15, 2020 ("Trace me on my cellphone, May 15, 2020")
- "Trace me on my cellphone", The Logic, May 14, 2020 ("Trace me on my cellphone, May 14, 2020")
- "Trace me on my cellphone", The Logic, May 13, 2020 ("Trace me on my cellphone, May 13, 2020")

"Tracking and tracing COVID: protecting privacy and data while using apps and biometrics", OECD, April 23, 2020, online: https://www.oecd.org/ coronavirus/en/policy-responses ("Tracking and tracing COVID: protecting privacy and data while using apps and biometrics").

"Tracking Ottawa's COVID-19 payouts", The Logic, June 4, 2020 ("Tracking Ottawa's COVID-19 payouts").

"Tracking people and events in real time while preserving privacy", Forbes Technology Council, May 21, 2020 ("Tracking people and events in real time while preserving privacy").

"Tracking the global response to COVID-19", Privacy International, https://privacyinternational.org/examples/tracking-global-response-covid-19 (accessed 20 May 2020) ("Tracking the global response to COVID-19").

"Trudeau announces COVID-19 tracking application", OpenMedia, email blast, June 19, 2020 ("OpenMedia: Trudeau announces COVID-19 tracking application").

"Trudeau leaves door open to using smartphone data to track Canadians' compliance with pandemic rules", CBC News, March 24, 2020, online: https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236 ("Trudeau leaves door open to using smartphone data to track Canadians' compliance with pandemic rules").

Tweets

- Tweets by Bianca, July 31-August 2, 2020 ("Bianca Wylie tweets, July 31-August 2, 2020").
- Tweet by Canadian Digital Service (CDS) re: COVID Alert Canada, August 3, 2020 ("Tweet by CDS, August 3, 2020")
- Tweet by CBC's Ontario provincial affairs reporter Mike Crawley re extension of Ontario's state of emergency, June 18, 2020, online: https://twitter.com/CBCQueensPark/status/1273675522376171520?s=20 ("Tweet by reporter Mike Crawley re extension of Ontario's state of emergency").
- Tweets by CDS CEO Aaron Snow, re: CDS/ODS work on COVID Alert Canada, July 31-August 2, 2020 ("Tweets by Aaron Snow, CDS CEO, July 31-August 2, 2020")
- Tweet by Michael Geist, July 31, 2020 ("Tweet by Michael Geist, July 31, 2020").
- Tweet by Shopify's Tobi Lutke r: COVID Alert Canada, August 7, 2020 ("Tweet by Shopify's Tobi Lutke, August 7, 2020").

"250 million Microsoft customer records exposed in latest breach", IT Governance, February 5, 2020, online: https://www.itgovernance.eu/blog/en/250-million-microsoft-customer-records-exposed-in-latest-breach ("250 million Microsoft customer records exposed in latest breach").

"Two security breaches affect health information of 211 people in Nova Scotia", Globe & Mail, August 4, 2020 ("Two security breaches affect health information of 211 people in Nova Scotia").

U

"U of G contact tracing app could help improve accuracy of the technology", University of Guelph News Release, June 19, 2020, online: https://news.uoguelph.ca/2020/06/u-of-g-contact-tracing-app-could-help-improve-accuracy-of-the-technology/ ("U of G contact tracing app could help improve accuracy of the technology").

"Uber offers COVID-19 contact tracing help amid chaotic U.S. response", reuters.com, July 20, 2020 ("Uber offers COVID-19 contact tracing help amid chaotic U.S. response").

"UK abandons contact-tracing app for Apple and Google model", The Guardian, June 18, 2020, online: https://www.theguardian.com/world/2020/jun /18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models ("UK abandons contact-tracing app for Apple and Google model").

"UK reported to be ditching coronavirus contacts tracing in favor of 'risk rating' app", August 6, 2020, TechCrunch, online: https://techcrunch.com/2020/08/06/uk-reported-to-be-ditching-coronavirus-contacts-tracing-in-favor-of-risk-rating-app/ ("UK reported to be ditching coronavirus contacts tracing in favor of 'risk rating' app").

"UK's newly-opened pubs may face data protection nightmare", Forbes, June 24, 2020, online: https://www.forbes.com/sites/emmawoollacott/2020/06/24/uks-newly-opened-pubs-may-face-data-protection-nightmare/#1bcb10fa76e9 ("UK's newly-opened pubs may face data protection nightmare").

"UK poised to abandon coronavirus app in favour of Apple and Google model", The Guardian, June 18, 2020 ("UK poised to abandon coronavirus app in favour of Apple and Google model").

"UPDATED: OPC now says it supports COVID-19 tracing app", The Wire Report, July 31, 2020 ("UPDATED: OPC now says it supports COVID-19 tracing app").

"UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app", The Wire Report, June 18, 2020 ("UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app").

"Update to our COVID-19 response", Salesforce blog, online: https://www.tableau.com/about/blog/2020/4/update-our-covid-19-response (dated April 14, 2020, accessed July 30, 2020) ("Salesforce – update to our COVID-19 response").

V

"Virginia rolls out first contact tracing app in US using Apple-Google tech", KHN, August 6, 2020, online: https://khn.org/morning-breakout/virginia-rolls-out-first-contact-tracing-app-in-us-using-apple-google-tech/ ("Virginia rolls out first contact tracing app in US using Apple-Google tech").

"Virus-tracing apps are rife with problems. Governments are rushing to fix them", The New York Times, July 8, 2020 ("Virus-tracing apps are rife with problems. Governments are rushing to fix them").

"Voluntary nationwide contact tracing app coming soon, says Trudeau", CBC News, June 18, 2020, online: https://www.cbc.ca/news/politics/contact-tracing-app-1.5617121 ("Voluntary nationwide contact tracing app coming soon, says Trudeau").

W

"What are the rules wrapping privacy during COVID-19?", Tech Crunch, March 20, 2020, online: https://techcrunch.com/2020/03/20/what-are-the-rules-wrapping-privacy-during-covid-19/ ("What are the rules wrapping privacy during COVID-19?").

"What digital contact tracing looks like around the world", The Spinoff (New Zealand), May 27, 2020, online: https://thespinoff.co.nz/tech/27-05-2020/what-digital-contact-tracing-looks-like-around-the-world/ ("What digital contact tracing looks like around the world").

"What ever happened to digital contact tracing?", Lawfareblog.com (Chas Kissick, Elliot Setzer, Jacob Schulz), July 21, 2020 ("What Ever Happened to Digital Contact Tracing?").

"What happens next? Covid-19 futures, explained with playable simulations", M. Salathé and N. Case, May 1, 2020, online: https://ncase.me/covid-19/ ("What happens next? Covid-19 futures, explained with playable simulations").

"What is coronavirus contact tracing and how important is it as Canada reopens?", Global News, May 22, 2020, online: https://globalnews.ca/news/ 6977095/coronavirus-contact-tracing-canada-reopens/ ("What is coronavirus contact tracing and how important is it as Canada reopens?")

"What is Salesforce?", Salesforce, online: https://www.salesforce.com/ca/products/what-is-salesforce/ (accessed July 30, 2020) ("What is Salesforce?").

"What is Shopify?", Shopify Blog (Shopify Staff), January 3, 2020, online: www.shopify.com/blog/what-is-shopify ("What is Shopify?").

"What Is Shopify & how does Shopify work?", Merchant Maverick (Liz Hull), April 21, 2020, online: www.merchantmaverick.com/what-is-shopify-and-how-does-shopify-work/ ("What Is Shopify & how does Shopify work?").

"What is the federal government's role in health care?", Healthy Debate, April 20, 2011, online: https://healthydebate.ca/2011/04/_mailpress_mailing_list_healthydebate-news/federal-role-health-care ("What is the federal government's role in health care?")

"Where is BC's COVID contact-tracing technology?", Business in Vancouver ("BIV"), August 14, 2020, online: https://biv.com/article/2020/08/where-bcs-covid-contact-tracing-technology ("Where is BC's COVID contact-tracing technology?").

"Who controls reins of Big Tech's COVID Alert app?", Toronto Star (Lisa Austin, David Lie, Wendy H. Wong), August 6, 2020 ("Who controls reins of Big Tech's COVID Alert app?").

"Why contact tracing apps will be the biggest test yet of data privacy versus public safety", Forbes, June 1, 2020, online: https://www.forbes.com/sites/bernardmarr/2020/06/01/why-contact-tracing-apps-will-be-the-biggest-test-yet-of-data-privacy-versus-public-safety/#7b547e914da2 ("Why contact tracing apps will be the biggest test yet of data privacy versus public safety").

"Why I Installed the COVID Alert App", Michael Geist blog, August 2, 2020 ("Why I Installed the COVID Alert App").

"Will the pandemic see Telus Health find its footing?", The Globe and Mail, June 7, 2020, online: https://www.theglobeandmail.com/business/article-will-the-pandemic-see-telus-health-find-its-footing/ ("Will the pandemic see Telus Health find its footing?")

"Will you download it?", The Logic, July 31 and August 4, 2020 ("Will you download it?").

"Workers around the world are already being monitored by digital contact tracing apps", buzzfeednews, May 30, 2020, online: https://www.buzzfeednews.com/article/carolinehaskins1/coronavirus-private-contact-tracing ("Workers around the world are already being monitored by digital contact tracing apps").

"Workplace privacy, an increasingly important issue in the Information Age", Minken Employment Lawyers, online: https://www.minkenemploymentlawyers.com/employment-law-issues/workplace-privacy-an-increasingly-important-issue-in-the-information-age/ ("Workplace privacy, an increasingly important issue in the Information Age").

X

N/A

Y

"Yes, Apple And Google have given us a serious contact tracing problem—here's why", Forbes (Zack Doffman, Cybersecurity), June 19, 2020, online: https://www.forbes.com/sites/zakdoffman/2020/06/19/how-apple-and-google-created-this-contact-tracing-disaster/#3d9815767ca2 ("Yes, Apple and Google have given us a serious contact tracing problem—here's why").

Z

N/A

ENDNOTES*

*Short-form citations only; for full citations, see Bibliography

[1] CPE Race to trace: security and privacy of COVID-19 contact tracing apps (emphasis added).

[2] See e.g., Digital contact tracing for pandemic response. DCTT is both network-level and application-level (i.e., contact tracing apps ["CTAs"]), which are specified where meant.

[3] Ontario launches consultations to strengthen privacy protections of personal data.

[4] S.C. 2000, ch. 5.

[5] R.S.C., 1985, c. P-21.

[6] Applications of digital technology in COVID-19 pandemic planning and response.

[7] COVI White Paper – Version 1.0, p. 3 (citations omitted).

[8] OECD policy responses to coronavirus (COVID-19): cities policy response.

[9] Cumulative confirmed COVID-19 deaths; Canada's coronavirus cases pass 120,000 as global total reaches 20 million (all numbers rounded).

[10] Health Canada Privacy Assessment.

[11] Applications of digital technology in COVID-19 pandemic planning and response.

[12] Applications of digital technology in COVID-19 pandemic planning and response.

[13] Applications of digital technology in COVID-19 pandemic planning and response.

[14] Applications of digital technology in COVID-19 pandemic planning and response.

[15] The case against lockdowns: can we fight the COVID-19 outbreak without confining people to their homes?

[16] CPE Race to trace: security and privacy of COVID-19 contact tracing apps (emphasis added).

[17] See e.g., recent studies published in The Lancet Infectious Diseases journal (finding contact tracing combined with isolation played a key role in controlling spread in Shenzen, China) and AMA Internal Medicine (examining Taiwan and concluding "[t]hese findings underscore the pressing public health need for accurate and comprehensive contact tracing and testing"), and World Health Organization ("WHO") (stating contact tracing is "an essential public health tool for controlling infectious disease outbreaks" that can "break the chains of transmission" of COVID-19): Canada has an army of volunteers ready to help fight COVID-19 – so why aren't we using them? (citing foregoing).

[18] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[19] This definition is grounded in definitions provided by experts such as Public Health Ontario and MIT Technology Review. See e.g., Public Health Ontario COVID-19 contact tracing initiative ("Contact tracing is a process that is used to identify, educate and monitor individuals who have had close contact with someone who is infected with a virus. These individuals are at a higher risk of becoming infected and sharing the virus with others. Contact tracing can help the individuals understand their risk and limit further spread of the virus."); A flood of coronavirus apps are tracking us (referring to identifying and notifying all those who come in contact with an infected person). The World Health Organization ("WHO") defined contact tracing as "identifying, accessing, and managing people who have been exposed to a disease to prevent onward transmission": Digital contact tracing: perspectives on approaches to COVID-19 (citing WHO).

[20] Joint statement on contact tracing, global scientists and researchers.

[21] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[22] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[23] Public Health Ontario COVID-19 contact tracing initiative.

[24] Public Health Ontario COVID-19 contact tracing initiative.

[25] Battling fast-moving COVID-19, Toronto's contact tracing system struggles to get up to speed (referencing Johns Hopkins University).

[26] Japan's contact-tracing method is old but gold (citing Japan's Ministry of Health, Labor and Welfare).

[27] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[28] Republican senators to introduce the COVID-19 Consumer Data Protection Act.

[29] See e.g., The security behind the NHS contact tracing app

[30] Japan's contact-tracing method is old but gold (noting Japan emphasized retrospective COVID-19 contact tracing in contrast to "most countries", which have prioritized prospective tracing).

[31] Japan's contact-tracing method is old but gold (citing official at Japan's Ministry of Health, Labor and Welfare).

[32] 'Shoe-leather' contact tracing works.

[33] What happens next? Covid-19 futures, explained with playable simulations.

[34] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive ("As we gradually open up our social and commercial institutions, it will be critical to monitor the contacts of those who have been tested positive for COVID-19.")

[35] COVI White Paper – Version 1.0, p. 3.

[36] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 8.

[37] Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app, slide 2.

[38] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[39] What ever happened to digital contact tracing?

[40] Privacy fears threaten New York City's coronavirus tracing efforts (citing Guillermo Chacon, founder of the Hispanic Health Network).

[41] Privacy fears threaten New York City's coronavirus tracing efforts (citing Jacqueline Seitz, staff attorney at the Legal Action Center, who advocates for privacy rights and anti-discrimination protections for those with HIV, AIDS, histories of substance use or criminal justice involvement).

[42] Privacy fears threaten New York City's coronavirus tracing efforts.

[43] Privacy fears threaten New York City's coronavirus tracing efforts.

[44] Privacy fears threaten New York City's coronavirus tracing efforts.

[45] What ever happened to digital contact tracing?

[46] Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app, slide 3; What is coronavirus contact tracing and how important is it as Canada reopens?

[47] Battling fast-moving COVID-19, Toronto's contact tracing system struggles to get up to speed.

[48] COVI White Paper – Version 1.0, p. 3.

[49] What is coronavirus contact tracing and how important is it as Canada reopens? (citing Canadian Medical Association president Dr. Sandy Buchman, who noted that "There's never been a pandemic in recorded history that didn't have a second wave, and often that second wave is even worse than the first").

[50] COVI White Paper – Version 1.0, p. 3.

[51] The security behind the NHS contact tracing app. Pre-COVID-19, broader "outbreak response" technology was deployed, for example, in 2019, in the Democratic Republic of Congo, for Ebola virus disease, using the Go.Data software application: WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[52] See e.g., What is coronavirus contact tracing and how important is it as Canada reopens? (referencing Canada's deputy chief public health officer Dr. Howard Njoo).

[53] Hard questions for policy-makers about digital contact tracing.

[54] Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app, slide 4.

[55] What happens next? Covid-19 futures, explained with playable simulations.

[56] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[57] Health Canada, as the "federal regulator of medical devices", defines "digital health technologies" to include "stand-alone software applications as well as integrated hardware and software systems which can utilize platforms, such as computers, smart phones, tables and wearables" (e.g., "wireless medical devices", "mobile medical apps", "telemedicine", and "software as medical device [SaMD]"): Notice: Health Canada's approach to digital health technologies.

[58] See e.g., Supreme Court of Canada decision raises interesting issues about jurisdiction over privacy-impactful technologies.

[59] Government efforts to track virus through phone location data complicated by privacy concerns.

[60] Government efforts to track virus through phone location data complicated by privacy concerns.

[61] Government efforts to track virus through phone location data complicated by privacy concerns.

[62] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 9 (emphasis added).

[63] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 9.

[64] Aka "wearable contact tracing technology".

[65] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?

[66] For example, Singapore's TraceTogether.

[67] For example, Alberta's ABTraceTogether, adapted from Singapore's TraceTogether (see details in body text below).

[68] See e.g., After COVID-19, will we live in a Big Brother world?

[69] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 47 (noting that to mitigate the risk of citizens using a third-party app, they should be clearly and explicitly informed about the link to download the official app).

[70] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive; COVID-19 contact tracing app are coming to a phone near you. How will we know whether they work?; WHO: Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing – Interim Guidance (CTAs "can only be effective in terms of providing data to help with the COVID-19 response when they are fully integrated into an existing public health system and national pandemic response. Such a system would need to include health services personnel, testing services and the manual contact tracing infrastructure").

[71] France offers a case study in the battle between privacy and coronavirus tracing apps (citing James Larus, part of the DP-PPT team and dean of the School of Computer and Communications Science at Switzerland's École Polytechnique Fédérale de Lausanne ["EPFL"] technical university).

[72] No, coronavirus apps don't need 60% adoption to be effective (citing Oxford Study spokesperson Andrea Stewart and the Study itself); Oxford Study. See also OPCC: Privacy review of the COVID Alert exposure notification application (citing the Study).

[73] After COVID-19, will we live in a Big Brother world? (referencing Singapore and Iceland as examples).

[74] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive.

[75] Carly Kind on contact-tracing apps.

[76] Workers around the world are already being monitored by digital contact tracing apps.

[77] COVI White Paper – Version 1.0, p. 3 (bracket added).

[78] See e.g., EC Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, para. 3.2; Privacy in the age of COVID: an IDAC investigation of COVID-19 apps (defining "symptom checker" as apps used by individuals to determine if they could have COVID-19, "telehealth" as apps used by individuals seeking COVID-19 healthcare treatment or services via their mobile device; and "quarantine administration" as apps used by governments to enforce quarantine and social distancing rules); CPE Race to trace: security and privacy of COVID-19 contact tracing apps (distinguishing between contact tracing apps and "other mobile technologies that have been developed or proposed to assist with the spread of COVID-19, including "self-diagnosis", "quarantine enforcement", and "aggregated data analytics"); After COVID-19, Will We Live in a Big Brother World? (referring to "QR pass", a downloadable, scannable QR code pass for non-infected or immune people to show third parties – such as police or store owners – they have permission to break quarantine); and Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19 (referring to "health passport"); WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance) (noting that symptom checkers can "include monitoring of breathing patterns using microphones in smart phones and the integration of wearable devices that monitor parameters such as oxygen saturation").

[79] Coronavirus statement.

[80] Surveys show conflicting support by Canadians for COVID-19 tracing app (emphasis added).

[81] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[82] The security behind the NHS contact tracing app (emphasis added).

[83] Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app, title slide and slides 3- 5, 10 (bracket added).

[84] EC Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection.

[85] See e.g., IDAC report on privacy and COVID-19 apps ("Contact tracing apps work by using location or proximity to identify and notify those that have been exposed to an infected individual. Location refers to the geographic location of the user. Proximity refers to the relationship between where the user is and where other users are…").

[86] See e.g., CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p.10 (referring to apps that use "a combination of" Bluetooth technology and location data); Norway's "Smittestopp" app; Mila's assessment of the "modified TraceTogether" app in its Discussion and outline of privacy and sociological concerns for CCTI iterations and features, p. 2.

[87] A mobile device ID ("device identification") is a distinctive string of numbers and letters associated with a mobile device, which is stored on the device.

[88] A flood of coronavirus apps are tracking us (first bracket added).

[89] Joint statement on contact tracing, global scientists and researchers.

[90] A flood of coronavirus apps are tracking us.

[91] Surveys show conflicting support by Canadians for COVID-19 tracing app; Anonymization by decentralization? The case of COVID-19 contact tracing apps; Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (bracket added) ("[These] apps will constantly broadcast unique, rotating Bluetooth codes that are derived from a cryptographic key that changes once each day. At the same time, they'll constantly monitor the phones around them, recording the codes of any other phones they encounter within a certain amount of range and time.")

[92] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered).

[93] Surveys show conflicting support by Canadians for COVID-19 tracing app; Anonymization by decentralization? The case of COVID-19 contact tracing apps; Does Covid-19 contact tracing pose a privacy risk? Your questions, answered; Carly Kind on contact-tracing apps.

[94] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[95] Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps.

[96] Surveys show conflicting support by Canadians for COVID-19 tracing app. An example of the former is Alberta's ABTraceTogether (see details below).

[97] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[98] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 11.

[99] Tracking people and events in real time while preserving privacy.

[100] Coronavirus contact-tracing: world split between two types of app.

[101] Tracking people and events in real time while preserving privacy.

[102] Coronavirus contact-tracing: world split between two types of app.

[103] Tracking people and events in real time while preserving privacy; Anonymization by decentralization? The case of COVID-19 contact tracing apps.

[104] Tracking people and events in real time while preserving privacy.

[105] Anonymization by decentralization? The case of COVID-19 contact tracing apps.

[106] Tracking people and events in real time while preserving privacy.

[107] Coronavirus contact-tracing: world split between two types of app.

[108] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? (emphasis added)

[109] Coronavirus contact-tracing: world split between two types of app.

[110] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? (emphasis added)

[111] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[112] Coronavirus contact-tracing: world split between two types of app.

[113] The security behind the NHS contact tracing app (modelled on UK's *original* app).

[114] COVI White Paper – Version 1.0, p. 3.

[115] France offers a case study in the battle between privacy and coronavirus tracing apps (citing James Larus, part of the DP-PPT team and dean of the School of Computer and Communications Science at Switzerland's École Polytechnique Fédérale de Lausanne ["EPFL"] technical university).

[116] France offers a case study in the battle between privacy and coronavirus tracing apps (emphasis and bracket added) (citing Bruno Sportisse, CEO of French research institute Inria).

[117] France offers a case study in the battle between privacy and coronavirus tracing apps.

[118] France's data protection watchdog reviews contact-tracing app StopCovid.

[119] See e.g., Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19.

[120] http://githubcom/DP-3T

[121] https://tcn-coalition.org. The TCN Coalition was founded in April 2020 and consists of "a global consortium of organizations dedicated to building privacy-first digital contact tracing apps", specifically COVID-19 exposure notification apps: Ibid and TCN Coalition applauds Apple and Google's digital contact tracing announcement. Its members include organizations that have developed apps based on the Apple/Google API (e.g., Covid Watch – see details below) and other protocols (e.g., NOVID): ibid and Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19.

[122] https://www.covid-watch.org/. Covid Watch, a US-based international non-profit, founded in February 2020 by researchers from Stanford (US) and Waterloo (Canada) universities, comprised of 500+ privacy and public health researchers, developers, volunteers, and academic advisers, developed the TCN Protocol (March 2020 , renamed from CEN Protocol), which influenced the Apple/Google API (used for its own Covid Watch app) as well as DP-3T and PACT: Ibid and Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19.

[123] https://pact.mit.edu/

[124] http://covidsafe.cs.washington.edu

[125] Joint statement on contact tracing, global scientists and researchers.

[126] https://tcn-coalition.org

[127] Privacy is not the problem with the Apple-Google contact-tracing toolkit.

[128] The world's first contact-tracing app using Google and Apple's API goes live.

[129] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? See also: Google - Exposure Notifications: Using technology to help public health authorities fight COVID-19 ("Only public health authorities can use this system", meaning "[a]ccess to the technology will be granted only to apps from public health authorities"; CTAs "will be developed by your local public health authority, not by Google or Apple",); additional citations below under "Google/Apple API".

[130] The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System.

[131] A flood of coronavirus apps are tracking us.

[132] The world's first contact-tracing app using Google and Apple's API goes live.

[133] Apple and Google's exposure notification system now publicly available.

[134] Google - About the Exposure Notification API update.

[135] New mobile app meant to help track COVID-19 in Ontario delayed.

[136] Google - About the Exposure Notification API update.

[137] Apple and Google's exposure notification system now publicly available.

[138] Apple and Google roll out their new exposure notification tool. Interest seems limited.

[139] Apple and Google's exposure notification system now publicly available; The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System.

[140] Google - COVID-19 exposure notification using Bluetooth low energy. See also animated infographic at: Google - Exposure notifications: using technology to help public health authorities fight COVID-19

[141] For Apple, see "Exposure notification APIs addendum (to the Apple developer program license agreement)", Apple, online: https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf (accessed July 26, 2020) ("Apple API Terms of Service"). For Google, see "Google COVID-19 exposure notifications service additional terms", Google, online: https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf (accessed July 26, 2020) ("Google API Terms of Service"). As noted below, the app developer is either the PHA itself or a PHA-authorized developer commissioned to create an app on the PHA's behalf, and the PHA must provide written documentation to the app review team at the Google/Apple app store: Google - Provide advance notice to the Google Play App Review team. In the latter case, the Terms permit the app developer to sign on behalf of the PHA, thereby binding the PHA: see e.g., Apple API Terms of Service ("developers endorsed or approved by a government entity must have a written agreement with such government entity that obligates the government entity to abide by the terms…")

[142] See e.g., Google API Terms of Service (app must be "endorsed by the relevant government public health authority [as confirmed by verifiable documentation").

[143] See e.g., Google API Terms of Service (app must be "published through Google Play by or on behalf of a government public health authority"); Apple API Terms of Service ("to use the…API, You must be a government entity, such as a government health services organization, or a developer who has been endorsed and approved by a government entity…").

[144] See e.g., See e.g., Google API Terms of Service (emphasis added) ("limited to one app per country unless the country has a regional approach, *or as otherwise permitted by Google*"); Apple API Terms of Service (emphasis added) (apps are limited to "one…per country unless the country has a regional approach, *or as otherwise agreed by Apple*"). See also: Apple, Google Covid-19 tool to be limited to one app per country; Privacy and COVID-19 mini-summit.

[145] See e.g., Google API Terms of Service (app "must provide end users with the ability to consent before using [it]" and "may not interfere with end users' ability to uninstall [it] or turn off notifications"); Apple API Terms of Service (app "must provide the user with the option to install to uninstall [it] and opt-out of receiving notifications…").
See also: Google - COVID-19 exposure notification using Bluetooth low energy ("Explicit user consent required")

[146] See e.g., Google API Terms of Service (app must be "used exclusively for COVID-19 response efforts and not for any other purpose, such as law-enforcement or any punitive action [e.g., individual quarantine enforcement]"); Apple API Terms of Service ("App … may be used only for the purpose of COVID-19 response efforts and not for any other purpose [such as law enforcement, including as enforced quarantine]").

[147] See e.g., Google API Terms of Service (emphasis added) (app that "provides an end user with an exposure notification…. *must* also provide post-exposure guidance and resources", which can include "clinical guidance and epidemiological information"); Apple API Terms of Service (emphasis added) (app "*should* contain current public health information on COVID-19, as well as references to the sources for any clinical information or guidance that may be provided").

[148] See e.g., Google API Terms of Service (app "may not require end users to provide personal data to obtain exposure notifications"); Apple API Terms of Service (app "may not require a user to enter user data to receive notifications of exposure").

[149] See e.g., Apple API Terms of Service (app "may only collect the minimum amount of user data necessary for COVID-19 response efforts and only with user consent [e.g., registration data may be collected with consent]").

[150] See e.g., Google API Terms of Service, Section 3(b)(i).

[151] See e.g., Google API Terms of Service (app "may only collect the minimum amount of end-user data necessary for COVID-19 response efforts and may only use the data for such efforts. All other uses [including selling or licensing such data using it to serve or target ads, or providing it to government agencies for purposes other than COVID-19 response) are prohibited"); Apple API Terms of Service ("any data collected… may be used only for the purpose of COVID-19 response efforts and not for any other purpose…"; "[n]either [developer nor app] may use or disclose data…for any purpose not related to COVID-19 response efforts, and any such use or disclosure must be with user consent"). See also: Google - COVID-19 exposure notification using Bluetooth low energy ("User controls all data they want to share, and the decision to share it")

[152] See e.g., Apple API Terms of Service ("You will not share any user data with Apple that users of Your Contact Tracing App may provide…").

[153] See e.g., Apple API Terms of Service ("You and Your Contact Tracing App may not use any data from the Exposure Notification APIs in a manner that would violate the legal rights of users [or any third parties] or otherwise be associated with systematic discrimination or marginalization, or provide a misleading, improper, or objectionable user experience or otherwise identify, or attempt to facilitate identification of, users who elect to not provide user data.")

[154] See e.g., Google - Exposure Notifications: Using technology to help public health authorities fight COVID-19 ("Your identity is not shared with other users, Google, or Apple"; "The system does not share your identity with other users, Apple, or Google. Public health authorities may ask you for additional information, such as a phone number, to contact you with additional guidance"); Google - COVID-19 exposure notification using Bluetooth low energy ("Bluetooth beacons and key don't reveal user identity or location"; "People who test positive are not identified to other users, Google, or Apple", "Will only be used for exposure notification by public health authorities for COVID-19 pandemic management").

[155] See e.g., Google API Terms of Service (emphasis added) ("app "may not … collect any device information to identify or track the *precise* location of end users"); Apple API Terms of Service (emphasis added) (app "may not use location-based APIs, may not use Bluetooth functionality [excluding Bluetooth functionality included in the Exposure Notification APIs] and may not collect any device information to identify the *precise* location of users"). See also:, Google - Exposure Notifications: Using technology to help public health authorities fight COVID-19 ("The Exposure Notification System doesn't track your location", means it "does not collect or use the location from your device"); Google - COVID-19 exposure notification using Bluetooth low energy ("Doesn't collect or use location data from your phone" and "Bluetooth beacons and key don't reveal user identity or location"); Apple and Google roll out their new exposure notification tool. Interest seems limited.

[156] See e.g., Google API Terms of Service, section 3(a)(i) and Google - Exposure notification cryptography specification preliminary — subject to modification and extension April 2020 v1.1; Apple API Terms of Service, section 3.4.

[157] Google - Exposure notification cryptography specification preliminary — subject to modification and extension April 2020 v1.1, p. 8.

[158] Google exec outlines privacy measures in new contact-tracing API (citing Google's head of public policy and government relations Colin McKay); Apple and Google roll out their new exposure notification tool. Interest seems limited.

[159] Google exec outlines privacy measures in new contact-tracing API.

[160] See e.g., Apple and Google roll out their new exposure notification tool. Interest seems limited.

[161] To enter the Google/Apple API Terms of Service the app developer must already have a Developer Agreement with Google/Apple: Google/Apple API Terms of Service, preambles and Apple API Terms of Service, section 4 (Submission to Apple for Apple Store Distribution).

[162] Apple API Terms of Service, section 4.

[163] Regulation (EU) 2016/679 (General Data Protection Regulation or "GDPR"), applicable as of May 25, 2018, in all member states to harmonize data privacy laws across Europe. It includes seven principles of data protection and eight privacy rights. For details, see: https://gdpr.eu/.

[164] See e.g., Google API Terms of Service, Section 3 Data Protection, Collection, and Privacy, ss. (b)(iv) (emphasis added).

[165] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[166] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance) (bracket added).

[167] Technology Theatre.

[168] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive.

[169] "False positives" are "notifications about exposures that didn't result in transmission of the disease" and "false negatives" are "failures to notify about exposure" for various reasons including "not everyone has a phone or will install the app": The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System. See also discussion in Part 1 and e.g.: COVID-19: When EU Tracking Apps Meet the Pandemic, Trust and Privacy by Design Are the Hosts; Hard questions for policy-makers about digital contact tracing (noting that Canada's chief public health officer, Dr. Theresa Tam, has "raised questions about the efficacy of digital contact tracing, citing false positives as one of several problems that can happen…"); Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (noting "there will be a false negative rate (…) based on everything from viruses left on surfaces rather than contact-based transmission to the fact that many groups of people either don't have smartphones or won't opt in to smartphone-based contact tracing").

[170] After COVID-19, Will We Live in a Big Brother World? (providing example of "a political rival or foreign agent using the app to spoil a political candidate's rally").

[171] See e.g., Hard questions for policy-makers about digital contact tracing (second bracket in original) (noting that "[w]orkers, rather than sick people, may ultimately become the target users of these [unreliable] apps as mechanisms to support their return to work, potentially increasing their exposure to the disease through the use of a novel technology that has known efficacy problems" and "[w]e know apps introduce bias through adoption. A number of civic technologies have proven that they tend to amplify the voices of those who are already connected."); After COVID-19, Will We Live in a Big Brother World? (noting that with contact tracing apps, "[i]f outbreaks occur in poorer neighbourhoods, which are more likely to be densely populated, intra-generational and, hence, prone to virus spread, these already vulnerable communities may face additional discrimination, stigmatization or socio-psychological harm" and app could create "different classes of those permitted to leave their homes and those who are not, based on political or loyalty-based factors")); Criminal Lawyers' Association position on digital COVID-19 contact tracing (noting concerns about "vigilantism, and other forms of discrimination against individuals and groups based on actual or perceived infection-status"); and Contact tracing must not compound historical discrimination (warning digital contact tracing could compound historical discrimination of minority groups).

[172] Telus to provide data from networks to Ottawa to help combat spread of COVID-19 (citing PIAC).

[173] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive.

[174] Joint statement on contact tracing, global scientists and researchers.

[175] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive.

[176] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive.

[177] Contact-tracing apps are a job for multipartisan leadership.

[178] Is digital contact tracing over before it began?

[179] See e.g., Coronavirus statement.

[180] See e.g.., Thinking through the manifold ramifications of collecting smartphone data for contact tracing; Coronavirus statement.

[181] See e.g.., Coronavirus statement.

[182] After COVID-19, Will We Live in a Big Brother World?

[183] See e.g.., Coronavirus statement.

[184] See e.g.., Coronavirus statement.

[185] See e.g.., Coronavirus statement; Telus to provide data from networks to Ottawa to help combat spread of COVID-19 (citing PIAC).

[186] Contact-tracing apps are a job for multipartisan leadership.

[187] Joint statement on contact tracing, global scientists and researchers.

[188] See e.g.., Coronavirus statement.

[189] See e.g.., Coronavirus statement.

[190] Empowering citizens against Covid-19 with an ML-based and decentralized risk awareness app, slide 5.

[191] After COVID-19, Will We Live in a Big Brother World?

[192] Joint statement on contact tracing, global scientists and researchers.

[193] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?; Government efforts to track virus through phone location data complicated by privacy concerns; Carly Kind on contact-tracing apps.

[194] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 10.

[195] 'Shoe-leather' contact tracing works.

[196] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 10.

[197] Ethical guidelines for COVID-19 tracing apps.

[198] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 10; See also UK poised to abandon coronavirus app in favour of Apple and Google model ("[T]he Bluetooth signal the app relies on to work is a very unreliable way of estimating distance…two phones kept in pockets on a crowded train can 'think' they are very far away from each other despite being within 2 metres, while two phones in active use outdoors can 'think' they are very close, even if they are fact well out of the danger zone".)

[199] 'Shoe-leather' contact tracing works.

[200] What ever happened to digital contact tracing?

[201] See e.g., Norway's "Smittestopp" app; Mila's assessment of the "modified TraceTogether" app in its Discussion and outline of privacy and sociological concerns for CCTI iterations and features, p. 2.

[202] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 10. A key example of a *non-contact tracing* location-based app is the Tim Horton's app reported in: "Double-double tracking: how Tim Hortons knows where you sleep, work and vacation" at https://business.financialpost.com/technology/tim-hortons-app-tracking-customers-intimate-data (see details below).

[203] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 10.

[204] A flood of coronavirus apps are tracking us.

[205] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, pp. 10-11.

[206] What ever happened to digital contact tracing?

[207] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?; Coronavirus contact-tracing: world split between two types of app; The world's first contact-tracing app using Google and Apple's API goes live.

[208] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?

[209] The world's first contact-tracing app using Google and Apple's API goes live.

[210] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[211] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (explaining that health care provider verification could be technologically enabled by providing a separate app to health care providers (e.g., doctors, nurses) that generates unique QR confirmation codes. "When doctors or nurses have determined that a patient is COVID-19 positive, they would tap a button to generate a confirmation code and give it to the patient, who then enters it into their (…) app. A representative from Apple and Google's joint contact tracing project said that their system similarly envisions that patients can't declare themselves infected without the help of a healthcare professional, who would likely confirm with a QR code.")

[212] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (citing University of Cambridge computer scientist and cryptographer Ross Anderson).

[213] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? (citing Marcel Salathé, an epidemiologist at the Swiss Federal Institute of Technology Lausannemwho is part of a team developing an international protocol for managing data in decentralized apps).

[214] France offers a case study in the battle between privacy and coronavirus tracing apps.

[215] See e.g., CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 12.

[216] Coronavirus contact-tracing: world split between two types of app; COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?

[217] Privacy is not the problem with the Apple-Google contact-tracing toolkit.

[218] Privacy is not the problem with the Apple-Google contact-tracing toolkit.

[219] France offers a case study in the battle between privacy and coronavirus tracing apps.

[220] The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System.

[221] Apple and Google roll out their new exposure notification tool. Interest seems limited.

[222] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[223] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?

[224] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[225] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[226] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[227] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 12.

[228] COVID-19 contact tracing must be ethical and responsible. Here's why.

[229] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered; CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 13.

[230] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (citing Ashkan Soltani, former chief technologist for the US Federal Trade Commission ["FTC"]).

[231] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[232] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered (underline added).

[233] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered; The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System (describing a correlation attack as: "someone set up a video camera to record the faces of people who passed by, while also running a rooted phone—one where the user has circumvented controls installed by the manufacturer—that gave the perpetrator direct access to the keys involved. Then […] when a COVID-positive key was broadcast over the network, the snoop could be able to correlate it with the face of a person captured on camera and use that to identify the COVID-positive individual.")

[234] Google promises privacy with virus app but can still collect location. See also: Bluetooth contact tracing apps built with Google and Apple's APIs still collect Android users' location data; Covid Tracker app throws spotlight on Google data harvesting.

[235] Google promises privacy with virus app but can still collect location.

[236] Google promises privacy with virus app but can still collect location; Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says.

[237] Google promises privacy with virus app but can still collect location.

[238] Google promises privacy with virus app but can still collect location.

[239] Google promises privacy with virus app but can still collect location.

[240] Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says.

[241] Covid Tracker apps throws spotlight on Google data harvesting (citing Google spokesperson).

[242] Switzerland launches SwissCovid tracing app for residents.

[243] Switzerland launches SwissCovid tracing app for residents (citing Matthew Dennis and Georgy Ishmaev, two researchers on the ethical aspects of emergent technologies and data at the Technical University of Delft).

[244] Privacy is not the problem with the Apple-Google contact-tracing toolkit.

[245] Privacy is not the problem with the Apple-Google contact-tracing toolkit (paragraph breaks deleted and emphasis added).

[246] Google promises privacy with virus app but can still collect location.

[247] Google promises privacy with virus app but can still collect location (bracket added).

[248] What digital contact tracing looks like around the world.

[249] Trace me on my cellphone, May 15, 2020 (emphasis added).

[250] What digital contact tracing looks like around the world.

[251] What ever happened to digital contact tracing?

[252] Government efforts to track virus through phone location data complicated by privacy concerns.

[253] Coronavirus contact-tracing: world split between two types of app.

[254] What ever happened to digital contact tracing?

[255] In Europe, as of August 5, 2020, more than 20 countries and territories have launched or plan CTAs, and most have chosen Bluetooth: Europe's coronavirus smartphone contact tracing apps.

[256] India's official app "Aarogya Setu" is mandated for certain populations only (e.g., workers in public and private offices, train travellers, and areas deemed high-risk for virus spread).

[257] See examples below under "decentralized Bluetooth (esp. Google/Apple API) apps".

[258] For example, the UK's *original* official app "NHSX Covid-19" (centralised Bluetooth risk assessment).

[259] See examples below under location-based apps.

[260] For example, Moscow and Saudi Arabia.

[261] For example, Iceland's official app "Rakning C-19", China's official app "Alipay Health Code" (location-based + data mining), Iran's official app ("Mask.ir"), Turkey's official app ("HayatEveSigar"), and Israel's official app ("HaMagen"). Some US states have deployed location-based official apps, including North and South Dakota ("Care19", renamed "Care19 Diary").

[262] For example, most of the above-noted 20 EU countries and territories that have deployed or adopted CTAs have chosen Bluetooth: Europe's coronavirus smartphone contact tracing apps.

[263] For example, Norway's official app "Smittestopp" (centralised Bluetooth + location [GPS]), now suspended, and India's official app "Aarogya Setu" (centralized Bluetooth + location [GPS]). As of mid-May 2020, globally 47 apps were deployed, of which 53% were location-based, 15% were proximity/Bluetooth-based, and 28% were both: After COVID-19, will we live in a Big Brother world?

[264] See e.g., What ever happened to digital contact tracing? ("[S]ome countries use a centralized model of data collection, where public health authorities can access the information collected by the apps, while others have gone with a decentralized version where data remains anonymized and is not shared with public health officials.")

[265] Bracelets, beacons, barcodes: wearables in the global response to COVID-19.

[266] What ever happened to digital contact tracing? (noting Salesforce built software for Rhode Island – largely for free – that helps the Department of Health with manual contact tracing – see details below).

[267] What ever happened to digital contact tracing? (noting Salesforce built software for Rhode Island – largely for free – that helps the Department of Health with manual contact tracing – see details below).

[268] Ottawa promotes contact tracing app for Canadians in fight against the spread of COVID-19 ("The app selected by the federal government is the same one unveiled by Ontario Premier Doug Ford shortly after the Prime Minister's announcement. It is a version of COVID Shield, an app created as an independent project by a team of developers affiliated with the Ottawa based e-commerce company Shopify"). See details below under "COVID Alert Canada".

[269] The US has no federal contact tracing program or official CTA. US contact tracing efforts vary from region to region; in some, the effort is coordinated at state level, while cities or counties take the lead in others: Uber offers COVID-19 contact tracing help amid chaotic U.S. response.

[270] What ever happened to digital contact tracing?

[271] COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?

[272] Coronavirus contact-tracing: world split between two types of app. Singapore offered the source code for TraceTogether free to other countries, and some (including Canada's Alberta government) developed it for their respective uses: Mobile contact-tracing app can help Alberta slow spread of COVID-19, top doctor says.

[273] See e.g., What ever happened to digital contact tracing? ("More than three months into the global pandemic, countries have begun to coalesce around a single model: Google and Apple's Bluetooth-based, decentralized API.")

[274] France backs virus tracing app following tough privacy debate.

[275] What ever happened to digital contact tracing?

[276] Yes, Apple and Google have given us a serious contact tracing problem—here's why (citing Minister-in-charge of the Smart Nation Initiative Vivian Balakrishnan, who explained that "Although a potential close contact would be notified by the system, there would be no way to identify how, when and whom the person was infected by or passed the infection to").

[277] 5 big EU countries blast Big Tech over approach to corona apps.

[278] Coronavirus contact-tracing: world split between two types of app.

[279] Europe's coronavirus smartphone contact tracing apps; Apple, Google release their joint technology for pandemic-tracking apps; Japan releases contact-tracing app using Apple and Google tech (updated); Saudi Arabia releases contact tracing app; England has started testing a contact tracing app – again. The originally-planned UK app could now be for England only, since other UK countries have their own official apps. No launch date for the new English app has been announced, but it is expected in winter 2020; the test phase started on August 13, 2020: England has started testing a contact tracing app – again; Northern Ireland launches UKs first Covid-19 contact-tracing app.

[280] What ever happened to digital contact tracing?; Trace me on my cellphone, July 22, 2020.

[281] Virginia rolls out first contact tracing app in US using Apple-Google tech (launched on August 5, 2020). North Dakota has two official apps, *location-based tracking* app "Care19", renamed "Care19 Diary" (launched first) and *Bluetooth decentralised (Google/Apple API)* "Care19 Alert" (launched second): Care19 Alert.

[282] Federal, Ontario governments launching apps to aid contact-tracing efforts (referencing Chris Parsons, senior research associate at the Citizen Lab at University of Toronto's Munk School of Global Affairs & Public Policy).

[283] Europe's coronavirus smartphone contact tracing apps.

[284] Coronavirus contact-tracing: world split between two types of app. DP-3T (decentralized privacy-preserving proximity) is an "*open-source protocol* for Bluetooth-based tracking in which an individual phone's contact logs are only stored locally, so no central authority can know who has been exposed": A flood of coronavirus apps are tracking us (emphasis added).

[285] French virus tracing app goes live amid debate over privacy.

[286] Coronavirus contact-tracing: world split between two types of app.

[287] Coronavirus contact-tracing: world split between two types of app. DP-3T (decentralized privacy-preserving proximity) is an "*open-source protocol* for Bluetooth-based tracking in which an individual phone's contact logs are only stored locally, so no central authority can know who has been exposed": A flood of coronavirus apps are tracking us (emphasis added).

[288] Ethical guidelines for COVID-19 tracing apps (citing Wiewiórowski, W. EU Digital Solidarity: A Call for a Pan-European Approach Against the Pandemic [European Data Protection Supervisor, 2020]); What ever happened to digital contact tracing?

[289] Switzerland launches SwissCovid tracing app for residents; EC: eHealth network guidelines to the EU member states and the European Commission on interoperability specifications for cross-border transmission chains between approved apps.

[290] What ever happened to digital contact tracing? (citing PM Johnson).

[291] What ever happened to digital contact tracing? (citing PM Johnson).

[292] What ever happened to digital contact tracing? (citing Professor Scassa's comments to reporters)).

[293] The Logic, Aug 4, 2020.

[294] Is a successful contact tracing app possible? These countries think so.

[295] Are contact-tracing apps helping tame the pandemic?

[296] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 16.

[297] Hard questions for policy-makers about digital contact tracing (bullets deleted, emphasis added) (noting "[i]n places like South Korea, Iceland and Singapore — the early adopters of contact tracing — the leaders of those programs have suggested that the technology hasn't been particularly helpful. More importantly, Hong Kong is the only place to have returned to public life without a significant increase in infections or a return to lockdown.")

[298] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 16.

[299] Lack of privacy oversight could hurt buy-in for COVID contact-tracing app, say critics; What ever happened to digital contact tracing? (noting Bahrain also exceeds 40%).

[300] What ever happened to digital contact tracing?; Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app; Despite Ontario delay, more provinces considering signing on with federal COVID Alert app.

[301] Contact-tracing apps are a job for multipartisan leadership. A key exception is Australia, "the only place to have hit its adoption target of 40 percent of smartphone users, (where) there are still significant concerns about failure rates: Notification: apps won't contain the outbreak of COVID-19.

[302] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[303] Europeans aren't really using COVID-19 contact-tracing apps.

[304] What ever happened to digital contact tracing?

[305] Europe proves contact-tracing apps aren't a coronavirus cure-all; Europeans aren't really using COVID-19 contact-tracing apps.

[306] What ever happened to digital contact tracing?

[307] Europeans aren't really using COVID-19 contact-tracing apps.

[308] Poland changed its official app from Bluetooth centralised (launched in April 2020) to decentralised (Google/Apple API) due to privacy concerns.

[309] See details below under "privacy risks".

[310] European Union: COVID-19: protecting personal data – the new normal.

[311] Majority of Americans say they won't use COVID contact tracing apps; 4 takeaways from contact tracing apps in other countries.

[312] Majority of Americans say they won't use COVID contact tracing apps.

[313] Majority of Americans say they won't use COVID contact tracing apps.

[314] Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic.

[315] Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic.

[316] Quality issues may be the stumbling block in the race for contact tracing apps.

[317] Quality issues may be the stumbling block in the race for contact tracing apps.

[318] Coronavirus contact-tracing: world split between two types of app (emphasis added).

[319] What ever happened to digital contact tracing?

[320] What ever happened to digital contact tracing?

[321] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 16.

[322] Hard questions for policy-makers about digital contact tracing (bullets deleted) (noting "[i]n places like South Korea, Iceland and Singapore — the early adopters of contact tracing — the leaders of those programs have suggested that the technology hasn't been particularly helpful. More importantly, Hong Kong is the only place to have returned to public life without a significant increase in infections or a return to lockdown.")

[323] What ever happened to digital contact tracing?

[324] Are contact-tracing apps helping tame the pandemic? (emphasis added).

[325] Hard questions for policy-makers about digital contact tracing (bullets deleted, emphasis added).

[326] Hard questions for policy-makers about digital contact tracing (bullets deleted, emphasis added).

[327] Hong Kong imposes strict COVID-19 measures, compulsory masks.

[328] Hard questions for policy-makers about digital contact tracing (bullets deleted) (noting "[i]n places like South Korea, Iceland and Singapore — the early adopters of contact tracing — the leaders of those programs have suggested that the technology hasn't been particularly helpful. More importantly, Hong Kong is the only place to have returned to public life without a significant increase in infections or a return to lockdown.")

[329] Europe proves contact-tracing apps aren't a coronavirus cure-all.

[330] Is a successful contact tracing app possible? These countries think so.

[331] Virus-tracing apps are rife with problems. Governments are rushing to fix them.

[332] Technology Theatre.

[333] What ever happened to digital contact tracing?

[334] What ever happened to digital contact tracing?

[335] What ever happened to digital contact tracing?

[336] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app; Coronavirus: Why Singapore turned to wearable contact-tracing tech.

[337] Trace me on my cellphone, May 27, 2020.

[338] What ever happened to digital contact tracing? See also: Coronavirus contact tracing apps were tech's chance to step up; One of the first contact tracing apps violates its own privacy policy

[339] Trace me on my cellphone, May 20, 2020.

[340] UK reported to be ditching coronavirus contacts tracing in favor of 'risk rating' app.

[341] Coronavirus app warning: StopCovid collects data of ANYONE near user in major system fault.

[342] What ever happened to digital contact tracing; Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.

[343] Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.

[344] What ever happened to digital contact tracing.

[345] Trace me on my cellphone, June 15, 2020.

[346] Data privacy laws collide with contact tracing efforts; privacy is prevailing.

[347] Google promises privacy with virus app but can still collect location.

[348] Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says.

[349] Google, Apple struggle to regulate Covid-19 tracing apps (brackets added).

[350] Bogus 'contact tracing' apps deployed to steal data: researchers.

[351] IDAC report on privacy and COVID-19 apps.

[352] Trace me on my cellphone, June 5, 2020; Google, Apple struggle to regulate Covid-19 tracing apps.

[353] Google, Apple struggle to regulate Covid-19 tracing apps.

[354] Coronavirus: how much does your boss need to know about you? (bracket added and paragraph breaks deleted)

[355] Coronavirus: how much does your boss need to know about you? (bracket added)

[356] Could this COVID-19 'health passport' be the future of travel and events?

[357] Aka "Tech Giants".

[358] Amazon, Apple, Facebook, and Google are the "Big Four" or "GAFA". There is power in numbers: on July 30, 2020, the Big Four released their quarterly earnings, including US$5 trillion (rough combined market capitalization), $773 billion (combined annual revenue), and $420 billion (combined total cash pile): The Logic, July 30, 2020; Big Tech's power, in 4 numbers.

[359] Palantir's NHS data project 'may outlive coronavirus crisis (noting: this initiative was announced by NHS' digital arm, NHSX, in March 2020; Palantir offered to provide data analysis services worth €88,000/week in return for a nominal fee of €1; and "a source close to the project said Palantir would be well placed to continue providing the service after the coronavirus outbreak comes to an end, especially if it was willing to provide its software for less than the market rate", which it might be willing to do in order to secure work globally with other PHAs).

[360] The tech 'solutions' for coronavirus take the surveillance state to the next level.

[361] The tech 'solutions' for coronavirus take the surveillance state to the next level (bracket added).

[362] See e.g., Carly Kind on contact-tracing apps.

[363] Privacy in the balance (paragraph breaks deleted).

[364] Big tech in healthcare: here's who wins and loses as Alphabet, Amazon, Apple, and Microsoft hone in on niche sectors of healthcare.

[365] Hospitals turn to big tech companies to store and analyze their data – leaving patients in the dark on privacy protections.

[366] Big tech in healthcare: here's who wins and loses as Alphabet, Amazon, Apple, and Microsoft hone in on niche sectors of healthcare.

[367] Germany takes on Big Tech: inside the fight to curb the power of global data giants.

[368] Google faces $5 billion lawsuit in US for tracking 'private' Internet use; Google sued for allegedly amassing user data, violating wiretap laws (noting this is a proposed class-action lawsuit and the class action might not be certified).

[369] Germany takes on Big Tech: inside the fight to curb the power of global data giants.

[370] Facebook exposed 87 Million users to Cambridge Analytica (noting the app offered personality quizzes).

[371] Surveillance Giants: how the business model of Google and Facebook threatens human rights; Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights (brackets added).

[372] Apple's empty grandstanding about privacy.

[373] Apple's empty grandstanding about privacy.

[374] Amazon refuses blame for Capital One data breach, says its cloud services were 'not compromised in any way'.

[375] Amazon refuses blame for Capital One data breach, says its cloud services were 'not compromised in any way'.

[376] Amazon refuses blame for Capital One data breach, says its cloud services were 'not compromised in any way'.

[377] Is ASW liable in Capital One breach?

[378] A data leak exposed the personal information of over 3,000 ring users.

[379] 250 million Microsoft customer records exposed in latest breach; Microsoft leaves 250M customer service records open to the Web.

[380] 250 million Microsoft customer records exposed in latest breach.
[381] Microsoft leaves 250M customer service records open to the Web.
[382] Microsoft leaves 250M customer service records open to the Web.
[383] Our health is all we have. But now Google wants it too.
[384] Bianca Wylie tweets, July 31-August 2, 2020.
[385] Four lessons: the digital health data.
[386] Four lessons: the digital health data.
[387] Four lessons: the digital health data.
[388] Four lessons: the digital health data (paragraph break deleted).
[389] Four lessons: the digital health data (bracket added).
[390] Four lessons: the digital health data.
[391] Four lessons: the digital health data.
[392] HealthCare.gov breach exposes data of 75K individuals; HealthCare.gov breach exposed personal details of 75,000 including partial Social Security numbers.
[393] At Mayo Clinic, sharing patient data with companies fuels AI innovation – and concerns about consent.
[394] At Mayo Clinic, sharing patient data with companies fuels AI innovation – and concerns about consent.
[395] Canadian government breaches exposed citizens' data: report; Personal data of more than 144K Canadians breached by federal government.
[396] Experts warn Canadians to brace for a new era of cyberthreats.
[397] Experts warn Canadians to brace for a new era of cyberthreats.
[398] Hospital 'overwhelmed' by cyberattacks fuelled by booming black market.
[399] Hospital 'overwhelmed' by cyberattacks fuelled by booming black market.
[400] Hospital 'overwhelmed' by cyberattacks fuelled by booming black market (bracket added).
[401] Hospital 'overwhelmed' by cyberattacks fuelled by booming black market (bracket added).
[402] After COVID-19, will we live in a Big Brother world?
[403] After COVID-19, will we live in a Big Brother world?
[404] After COVID-19, will we live in a Big Brother world?
[405] Covid-19 tracking apps, or: how to deal with pandemic most unsuccessfully.
[406] Canada's privacy watchdogs see uptick in work amid pandemic (emphasis added).
[407] Canada's privacy watchdogs see uptick in work amid pandemic.
[408] Canada's privacy watchdogs see uptick in work amid pandemic (citing blog post).
[409] Public Health Agency of Canada – FAQ.
[410] Public Health Agency of Canada – FAQ.
[411] Public Health Agency of Canada – FAQ (emphasis added).
[412] Public Health Agency of Canada – FAQ (emphasis added).
[413] Public Health Agency of Canada – FAQ (bullets deleted and brackets added).
[414] Canada: legal responses to health emergencies.
[415] Canada: legal responses to health emergencies.
[416] Canada: legal responses to health emergencies.
[417] Canada: legal responses to health emergencies.
[418] Canada's health care system.
[419] Canada's health care system.
[420] Canada's health care system. The *Canada Health Act* sets out the principles that provincial health plans must adhere to in order to receive federal transfers *without penalty*: What is the federal government's role in health care?
[421] Privacy experts support call for national plan for COVID-19 contact tracing app.
[422] Public Health Agency of Canada – FAQ.
[423] Public Health Agency of Canada – FAQ. The Canadian Public Health Association self-describes as "the independent national voice and trusted advocate for public health, speaking up for people and populations to all levels of government": https://www.cpha.ca/
[424] Public Health Agency of Canada – FAQ.
[425] Public Health Agency of Canada – FAQ.
[426] Canadian Network for Public Health Intelligence.
[427] Alberta reports 49 new COVID-19 cases, one additional death.

[428] On May 20, 2020, Telus announced its "Data for Good" program to "provide de-identified network mobility data and insights to government researchers at the Natural Sciences and Engineering Council of Canada (NSERC) in support of COVID-19 research" , free of charge, to "prevent or mitigate future phases of COVID-19 or other pandemics": TELUS Data for Good program to provide de-identified network mobility data and insights to the Natural Sciences and Engineering Research Council of Canada in support of COVID-19 research. NSERC is the largest funder of natural science and engineering research in Canada and, in response to COVID-19, NSERC is providing up to $15M in total support to stimulate collaborations between academic researchers, the public and not-for-profit sectors, and industry to address pandemic-related research: Telus to provide network mobility data and insights in support of Covid-19 research. Additional network level initiatives are under development, such as Telus group tracking (for details, see: How mobile phones could help trace the spread of COVID infections) and potential initiatives by BCE Inc. and Rogers Communications Inc. (for details, see: Telus to provide data from networks to Ottawa to help combat spread of COVID-19).

[429] Trudeau leaves door open to using smartphone data to track Canadians' compliance with pandemic rules.

[430] Group of Shopify volunteers create free COVID-19 contact tracing app; Ottawa-based Shopify volunteers to launch COVID-19 exposure notification solution; Plans for single COVID-19 contact tracing app facing resistance: health minister.

[431] Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps; Trace me on my cellphone, May 28, 2020; Privacy experts support call for national plan for COVID-19 contact tracing app (citing Ontario Premier Ford, "We need a national plan for contact tracing. Right now each individual province is doing it, but we need a national plan … It's absolutely critical").

[432] Privacy experts support call for national plan for COVID-19 contact tracing app**.**

[433] Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app; Plans for single COVID-19 contact tracing app facing resistance: health minister.

[434] Health Minister details pushback towards potential Canada-wide COVID-19 contact tracing app.

[435] PM Trudeau tweet, June 18, 2020 ("That's why we've been working why we've been working with @CDS_GC, @Shopify, @BlackBerry, and @ONGov to develop an app…)

[436] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure; Logic Briefing: Northern exposure notification; UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[437] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure (not naming the federal app or its foundational app).

[438] Ontario Enhancing COVID-19 case and contact management. Initial media reports confirmed that "it's unclear if the app will also be called COVID Alert outside Ontario": Shopify, Blackberry, and Ontario to help Canada launch contact tracing app.

[439] In contrast, FPT privacy commissioners refer to "federal aspects" and "Ontario components" of the "COVID Alert app". See e.g., Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert.

[440] Federal, Ontario governments launching apps to aid contact-tracing efforts. The PMO news release does not mention COVID Shield by name but rather states CDS is "leading the development of the app, in collaboration with" ODS "and building upon technology developed by Shopify volunteers": Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure. However, media reports confirm the app is built on COVID Shield, for example: COVID-19 tracing app starts beta testing after three-week delay ("The government of Canada's national contact tracing app is built on COVID Shield…"); "Shopify, Blackberry, and Ontario to help Canada launch contact tracing app ("The new app… is built on top of COVID Shield…").

[441] COVID Shield website; Trace me on my cellphone, May 28, 2020; Shopify volunteers release open-sourced contact-tracing app; Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert (noting that as of May 2020, the Ontario government was developing an Ontario-specific "exposure notification app (known at that time as COVID Shield)", which was replaced by a national app "spearheaded by the federal government, in coordination with provincial and territorial governments").

[442] Despite Ontario delay, more provinces considering signing on with federal COVID Alert app.

[443] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[444] Federal, Ontario governments launching apps to aid contact-tracing efforts (noting a federal government source said COVID Shield Canada will work throughout all PTs, some of whom may choose to adopt it).; Coronavirus contact-tracing app to launch nationally in early July, Trudeau says (referring to Minister Freeland).

[445] Federal, Ontario governments launching apps to aid contact-tracing efforts.

[446] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.

[447] PM says a national contact tracing app is coming next month, how will it work? (citing PM "It will be one app that whether you download it and live in Ontario and travel to B.C. or travel to the Northwest Territories— if that becomes an option—it will work everywhere across the country. So, it's one app for all Canadians"); PM Trudeau's televised announcement of national contact tracing app and subsequent Q&A, June 18, 2020; UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[448] COVID-19 tracing app starts beta testing after three-week delay.

[449] Making coronavirus contact-tracing app user-friendly caused delay, Hajdu says (citing Minister Hajdu).

[450] Despite Ontario delay, more provinces considering signing on with federal COVID Alert app.

[451] COVID-19 tracing app starts beta testing after three-week delay.

[452] Only 29 percent of Canadians are 'very likely' to download COVID Alert app.

[453] Tweets by Aaron Snow, CDS CEO, July 31-August 2, 2020.

[454] Download COVID Alert today.

[455] Download COVID Alert today.

[456] Can't download the COVID Alert app? Your operating system may be too old (or new) (citing PM Trudeau).

[457] Will you download it?

[458] Download COVID Alert today. When OPCC asked GoC what would be the specific benefits of the app for residents of PTs whose government has not adopted it, GoC explained the app could help permit safe interprovincial travels (e.g., if a user in a participating jurisdiction travels to another PT that is not yet participating, and subsequently tests positive for COVID-19, users in that jurisdiction can still be notified of potential exposure): OPCC: Privacy review of the COVID Alert exposure notification application.

[459] OPCC: Privacy review of the COVID Alert exposure notification application; COVID Alert app could result in some people being ID'd.

[460] Ottawa plans up to $10 million for COVID Alert public awareness campaign (citing Minister Murray).

[461] Alberta will switch over to national coronavirus tracing app; Alberta to adopt national COVID-19 exposure app.

[462] Canada's population has grown to nearly 38 million: Stats Can; Can't download the COVID Alert app? Your operating system may be too old (or new) (citing PM Trudeau).

[463] PM says a national contact tracing app is coming next month, how will it work?"

[464] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[465] PM Trudeau's televised announcement of national contact tracing app and subsequent Q&A, June 18, 2020.

[466] Can't download the COVID Alert app? Your operating system may be too old (or new).

[467] Ottawa plans up to $10 million for COVID Alert public awareness campaign, Aug 7, 2020.

[468] Ottawa plans up to $10 million for COVID Alert public awareness campaign (citing Minister Murray).

[469] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[470] PM says a national contact tracing app is coming next month, how will it work?

[471] PM says a national contact tracing app is coming next month, how will it work?

[472] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[473] Coronavirus tracing app not yet OK'd by privacy watchdog, but outside experts give thumbs up. In an emailed statement to media, an OPCC spokesperson said: "We were recently contacted by Health Canada about a COVID-19 exposure notification application. We have requested and are awaiting necessary information and, until such time as we receive that information, we have not provided our recommendations to the government. We are working diligently and responsibly to develop that advice.": UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app.

[474] COVID Alert Privacy Notice (Exposure Notification).

[475] News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness ("the Office of the Privacy Commissioner of Canada [OPC] and the Office of the Information and Privacy Commissioner of Ontario [IPC] have concluded their review of the COVID Alert exposure notification application and support use of the app"); OPCC: Privacy review of the COVID Alert exposure notification application; Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert.

[476]Health Canada Privacy Assessment.

[477] OPCC and the Ontario Privacy Commissioner "coordinated our respective reviews of the privacy-related aspects of the COVID Alert app, each from our respective perspective and jurisdictions" and "guided by the privacy principles enunciated in the Joint Statement by Federal, Provincial and Territorial Privacy Commissioners". The Ontario Commissioner's review was informed by Ontario-specific documents including a provincial PIA dated July 24, 2020, and MOU between GoC and the Ontario government dated July 30, 2020: Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert.

[478] News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness.

[479] Office of the Information and Privacy Commissioner of Ontario Recommendations on COVID Alert.

[480] News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness.

[481] Health Canada Privacy Assessment.

[482] For example, Michael Geist, University of Ottawa law professor and Canada Research Chair in Internet and E-commerce Law said COVID Alert Canada is "a low risk, low reward approach" and Michael Bryant, Executive Director of the Canadian Civil Liberties Association said "it's not terrible" and "time will tell" whether "it will work as advertised": Tweet by Michael Geist, July 31, 2020; Federal COVID-19 app launches after month-long delay (citing Bryant).

[483] News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness.

[484] Ottawa plans up to $10 million for COVID Alert public awareness campaign.

[485] Ottawa plans up to $10 million for COVID Alert public awareness campaign.

[486] Examples include the UK (*alternative* official app) and North Dakota (*additional* official app) (see details above under "Global DCTT").

[487] See e.g., COVID-19 exposure notification app now available ("Canada could end up with a patchwork of applications being used across the country and, as a result, limited efficacy when it comes to interprovincial spread").

[488] Privacy experts support call for national plan for COVID-19 contact tracing app.

[489] Plans for single COVID-19 contact tracing app facing resistance: health minister.

[490] Trace me on my cellphone, June 5, 2020.

[491] COVID-19 tracing app starts beta testing after three-week delay.

[492] Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app.

[493] Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app; Tracking Ottawa's COVID-19 payouts.

[494] Contact tracing apps may help slow the spread of COVID-19. But will privacy concerns prevent Canadians from using them?

[495] ABTraceTogether FAQ; Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps; Mobile contact-tracing app can help Alberta slow spread of COVID-19, top doctor says; Privacy expert says flawed Alberta COVID-19 contact tracking app shouldn't have been released.

[496] Mobile contact-tracing app can help Alberta slow spread of COVID-19, top doctor says.

[497] Federal, Ontario governments launching apps to aid contact-tracing efforts.

[498] Alberta reports 49 new COVID-19 cases, one additional death; Contact tracing apps may help slow the spread of COVID-19. But will privacy concerns prevent Canadians from using them?

[499] Testing the public's trust: Quebec premier mulls adopting contact-tracing app.

[500] Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app.

[501] Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps.

[502] Privacy experts support call for national plan for COVID-19 contact tracing app**.**

[503] Federal government rules out adoption of Mila Institute's COVID-19 contact-tracing app.

[504] OPH contact tracing tech on hold while province and feds develop their own.

[505] New Brunswick's plan for COVID-19 contact tracing pp thwarted by federal government; Province's plan for COVID-19 contact-tracing app denied by Ottawa.

[506] COVID Alert, federally backed contact tracing app, hints at what Manitobans may be able to expect (citing an email from an unnamed Manitoba government spokesperson).

[507] See e.g., Alberta to adopt national COVID-19 exposure app.

[508] Alberta will switch over to national coronavirus tracing app; Alberta to adopt national COVID-19 exposure app; Here's your daily COVID-19 roundup, July 14, 2020.

[509] Commissioner releases report on ABTraceTogether contact-tracing app. The report presents the Alberta Commissioner's findings on its review of the app's privacy impact assessment ("PIA"), which was submitted by Alberta Health ("AH") and endorsed by Alberta Health Services ("AHS"), as required by Alberta's *Health Information Act* ("HIA"). In particular, the report accepted the PIA with recommendations, including: to clarify inconsistencies between the PIA and publicly available information; and to continue to report publicly on the app's use and effectiveness and AH's plans to dismantle the app "when the time comes": Ibid.

[510] Despite Ontario delay, more provinces considering signing on with federal COVID Alert app; Ottawa plans up to $10 million for COVID Alert public awareness campaign.

[511] COVID-19 tracing: a Quebec application "ready in a few weeks" (citing Mila president and CEO Valérie Pisano).

[512] P.E.I. to see how COVID-19 app fares in Ontario before final decision on use.

[513] Alberta will switch over to national coronavirus tracing app; Alberta to adopt national COVID-19 exposure app; Ottawa plans up to $10 million for COVID Alert public awareness campaign; Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook.

[514] Health Canada Privacy Assessment.

[515] Little enthusiasm among Quebec politicians as government mulls COVID-19 tracing app; COVID-19 tracing: a Quebec application "ready in a few weeks".

[516] Quebec Assembly signals possible split from COVID Alert system; Opposition parties says COVID-19 tracing app is a non-starter (citing Québec solidaire co-spokesperson Gabriel Nadeau-Dubois).

[517] Quebec launches online consultation for COVID-19 contact tracing app.

[518] Where is BC's COVID contact-tracing technology? (bracket added).

[519] According to media reports, prior to Alberta's official adoption of COVID Alert Canada, it was pressing GoC to help ensure the two apps could work together: Alberta to adopt national COVID-19 exposure app.

[520] Voluntary nationwide contact tracing app coming soon, says Trudeau.

[521] Tweet by CDS, August 3, 2020; Ottawa plans up to $10 million for COVID Alert public awareness campaign; Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[522] Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook; Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[523] EDITORIAL: Are you up for the COVID contact-tracing app?; Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[524] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[525] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app (bracket added).

[526] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app; Coronavirus: the great contact-tracing apps mystery (noting the Irish app, during the installation process, asks users to consent to collection of "anonymous metrics" about the "effectiveness of contact-tracing processes").

[527] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[528] OpenMedia CTA petition; OpenMedia: Trudeau announces COVID-19 tracking application.

[529] Expectations: OPC's guide to the privacy impact assessment process (citing "2018-19 Survey of Canadians on Privacy", online: https://priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#toc1-3.).

[530] Report finds massive drop in Canadians' willingness to disclose personal information for free online services.

[531] Majority of Canadians do not approve of a mandatory contact tracing app: Mainstreet poll.

[532] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[533] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[534] Surveys show conflicting support by Canadians for COVID-19 tracing app.

[535] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 13.

[536] Canadians' security and privacy must be protected in the race to trace; Ryerson cyber-policy group calls for law preventing employers and businesses making contact-tracing app mandatory

[537] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 14 (square brackets added).

[538] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 14.

[539] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 14.

[540] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, pp. 4, 14-15.

[541] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 15 ("Recommendation: Contact tracing apps should be voluntary, fully opt-in and require informed consent. The federal, provincial and territorial governments should pass legislation to ensure public and private entities cannot make it mandatory to have access to the app in order to access goods, services, employment or housing.")

[542] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 13.

[543] Federal COVID-19 app launches after month-long delay.

[544] The Logic, August 10, 2020; Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[545] Quebec Assembly signals possible split from COVID Alert system.

[546] Misconceptions persist about effectiveness and privacy of Canada's COVID Alert app.

[547] EDITORIAL: Are you up for the COVID contact-tracing app?

[548] Defined as the act of bringing data into an app from an external source, which can be the subject of the data (i.e., the user) or a third party.

[549] "Processing" is "use" under PIPEDA. PIAC acknowledges that in global privacy discourse, "processing" is often treated as a discrete function and/or used as an umbrella term for "collecting, using, and sharing".

[550] "Data matching" is "the creation of new information by combining two or more sets of data", which "can pose privacy risks, for example, unintended inferences may be made about individuals whose data is matched, or previously anonymous data may become identifiable" ("re-identification of anonymised data"): Alberta OIPC: Privacy impact assessment requirements, pp. 11, 27, 31.

[551] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 13 (defining "function creep" as "use of technology beyond that for which it was originally intended").

[552] Aka "sharing", "access", "transfer".

[553] Aka "storage" versus "deletion/disposal".

[554] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 12.

[555] "Data security is an essential element of privacy protection" because "information is not private if entities that shouldn't have access to it can steal it": Brookings Report, Bridging the gaps: a path forward to federal privacy legislation, pp. 46, 49.

[556] Aka "disclosure".

[557] For this use of "notifications" and "privacy statement/policy", see e.g., Brookings Report, Bridging the gaps: a path forward to federal privacy legislation, p. 67.

[558] Explicit/implicit (aka "express/implied") is used distinctly (not synonymously) with opt-in/out. Opt-in and out are not themselves consent, rather they are methods to try to generate proof of explicit or implicit consent.

[559] See e.g., Alberta OIPC: Privacy impact assessment requirements, p. 22.

[560] See e.g., Alberta OIPC: Privacy impact assessment requirements, pp. 14 (referring to "flow analysis") and 22 ("information flow analysis").

[561] Notification: apps won't contain the outbreak of COVID-19.

[562] News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19.

[563] COVID-19 exposure notification app now available.

[564] Health Canada Privacy Assessment (bracket added).

[565] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.
[566] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.
[567] News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19 (bracket added).
[568] Tweets by Aaron Snow, CDS CEO, July 31-August 2, 2020.
[569] What is Shopify?
[570] What Is Shopify & how does Shopify work?
[571] Shopify POS review.
[572] Shopify POS review.
[573] The invisible selling machine.
[574] Snap has a new partnership that opens it up to hundreds of thousands of advertisers.
[575] Health ecommerce: serving and selling wellness in a jaded online world.
[576] Despite Ontario delay, more provinces considering signing on with federal COVID Alert app.
[577] BlackBerry CEO says the mobile company's turnaround has hit a tipping point after near-death experience.
[578] BlackBerry Ltd (BB.TO), https://www.reuters.com/companies/BB.TO.
[579] BlackBerry solutions for healthcare providers.
[580] BlackBerry healthcare momentum continues with latest HIMSS INFRAM certification.
[581] Blackberry and how automotive AI could revolutionize healthcare.
[582] Federal, Ontario governments launching apps to aid contact-tracing efforts.
[583] Privacy and security are key to contact tracing apps.
[584] Health Canada Privacy Assessment, including footnote 3 (bracket in original).
[585] OPCC: Privacy review of the COVID Alert exposure notification application.
[586] Accessibility statement for COVID Alert.
[587] Can't download the COVID Alert app? Your operating system may be too old (or new) (first quote cited to CDS tweet dated July 31, 2020).
[588] Ottawa plans up to $10 million for COVID Alert public awareness campaign.
[589] See e.g., Ottawa plans up to $10 million for COVID Alert public awareness campaign.
[590] COVID Alert app one of many tools in fight against coronavirus, Dr. Tam says.
[591] Ottawa plans up to $10 million for COVID Alert public awareness campaign.
[592] Less than 4% of Canadians have the COVID Alert tracing app — despite better privacy protection than Facebook.
[593] New COVID-19 notification app rolls out in Ontario.
[594] Potential privacy threat to Android owners using COVID exposure notification app won't be fixed until 'later in the third quarter'.
[595] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app (citing PM) (emphasis added).
[596]Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.
[597] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app (emphasis added).
[598] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app (citing PM).
[599] Coronavirus contact-tracing app to launch nationally in early July, Trudeau says (citing federal officials).
[600] Federal, Ontario governments launching apps to aid contact-tracing efforts.
[601] Coronavirus contact-tracing app to launch nationally in early July, Trudeau says (citing federal officials).
[602] Federal, Ontario governments launching apps to aid contact-tracing efforts.
[603] Download COVID Alert today.
[604] Download COVID Alert today.
[605] Health Canada Privacy Assessment.
[606] COVID Alert Privacy Notice (Exposure Notification).
[607] Company announcements: an update on exposure notifications; Android 11 release date: when can you expect it to launch?
[608] COVID Alert: Exposure notification application privacy assessment.
[609] Continuously improving COVID Alert.
[610] COVID Alert: Exposure notification application privacy assessment.
[611] See Appendix of Screenshots.
[612] COVID-19 roundup: Ontario delays its virus exposure-notification app launch (emphasis added) (citing Ontario government official).
[613] See Appendix of COVID Alert Canada Screenshots.
[614] Frequently asked questions about the Corona-Warn-App: what do the exposure check logs show?
[615] Frequently asked questions about the Corona-Warn-App: what do the exposure check logs show?

[616] Continuously improving COVID Alert.
[617] COVID Alert app could result in some people being ID'd.
[618] OPCC: Privacy review of the COVID Alert exposure notification application.
[619] COVID Alert: Exposure notification application privacy assessment.
[620] Ottawa plans up to $10 million for COVID Alert public awareness campaign.
[621] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.
[622] COVID-19 Exposure Notification App Advisory Council.
[623] Terms of Reference of the Advisory Council to federal, provincial and territorial governments on the national COVID-19 exposure notification app.
[624] Canadian privacy watchdogs support COVID-19 exposure app.
[625] Privacy review of the COVID Alert exposure notification application.
[626] Exposure notification: Diagnosis Server implementation.
[627] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app (citing PM).
[628] Prime Minister announces new mobile app to help notify Canadians of COVID-19 exposure.
[629] UPDATED – Privacy commissioner hasn't approved new gov't contact tracing app (citing PM).
[630] Speech: Prime Minister's remarks on COVID-19 measures and the launch of the COVID Alert national application.
[631] News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19.
[632] COVID-19 exposure notification app now available.
[633] Health Canada Privacy Assessment (e.g., app is "designed to minimize collection and storage of personally identifiable information", " is unlikely to involve the collection of any personally identifiable information", and "would not transmit PII to the key server").
[634] Coronavirus contact-tracing app to launch nationally in early July, Trudeau says.
[635] COVID Alert Privacy Notice (Exposure Notification).
[636] See Appendix of screenshots.
[637] COVID Alert: Exposure notification application privacy assessment.
[638] COVID Alert: Exposure notification application privacy assessment.
[639] COVID Alert: Exposure notification application privacy assessment.
[640] COVID Alert: Exposure notification application privacy assessment.
[641] Determine appropriate retention for network logs #199.
[642] Determine appropriate retention for network logs #199.
[643] COVID Alert: Exposure notification application privacy assessment.
[644] COVID Alert: Exposure notification application privacy assessment.
[645] Privacy review of the COVID Alert exposure notification application.
[646] COVID Alert: Exposure notification application privacy assessment.
[647] Health Canada Privacy Assessment, "One-time codes, IP addresses, API tokens and HashIDs".
[648] COVID Alert: Exposure notification application privacy assessment.
[649] COVID Alert: Exposure notification application privacy assessment.
[650] COVID Alert: Exposure notification application privacy assessment.
[651] COVID Alert: Exposure notification application privacy assessment.
[652] COVID Alert: Exposure notification application privacy assessment.
[653] COVID Alert: Exposure notification application privacy assessment.
[654] Health Canada Privacy Assessment.
[655] Ontario Enhancing COVID-19 case and contact management.
[656] Ottawa plans up to $10 million for COVID Alert public awareness campaign.
[657] Continuously improving COVID Alert.
[658] COVID Alert Portal for healthcare providers.
[659] COVID-19 test results website Terms of Use.
[660] COVID Alert: Exposure notification application privacy assessment.
[661] COVID-19 exposure notification app now available.
[662] COVID Alert: Exposure notification application privacy assessment.
[663] See Appendix A,

[664] News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19.

[665] Shopify, Blackberry, and Ontario to help Canada launch contact tracing app.

[666] COVID Alert: Exposure notification application privacy assessment.

[667] COVID Alert: Exposure notification application privacy assessment.

[668] OPCC: Privacy review of the COVID Alert exposure notification application.

[669] Experts say Sask could be more transparent with COVID-19 data without sacrificing privacy.

[670] Coronavirus disease (COVID-19): Travel restrictions, exemptions and advice.

[671] Canada-US border will remain closed until September 21.

[672] Coronavirus disease (COVID-19): Travel restrictions, exemptions and advice.

[673] News Release: Conservatives request Privacy Commissioner investigate federal contact tracing app and ArriveCAN app (also requesting a review of COVID Alert Canada). The Conservative MPs are: Hon. Michelle Rempel Garner, Shadow Minister for Industry and Economic Development, Pierre Paul-Hus, Shadow Minister for Public Safety, Border Security, and Emergency Preparedness, and Matt Jeneroux, Shadow Minister for Health.

[674] UPDATED: OPC now says it supports COVID-19 tracing app.

[675] Ontario's construction industry pushes for wearable COVID-19 tracing app (citing Premier Ford); 1 million downloads in 5 weeks - the tech company fighting COVID in Canada (describing TraceScan as "a made-in-Ontario *app that includes wearables* and features technology that can be worn on a bracelet or carried in a wallet" and noting that Bradley Metlin, spokesperson for Ontario Labor Minister Monte McNaughton, told the Globe & Mail: "We continue to encourage the federal government to engage companies like Facedrive… who are coming forward with made-in-Ontario/Canada solutions to keep all workers safe").

[676] Ontario's construction industry pushes for wearable COVID-19 tracing app; 1 million downloads in 5 weeks - the tech company fighting COVID in Canada. On July 29, 2020, Facedrive announced that *"TraceSCAN Wearables*, Facedrive Health's COVID-19 contact tracing wearable solution" is "launching a pilot project" with LiUNA in early August: Facedrive launches TraceSCAN Wearables pilot project in partnership with Labourers' International Union of North America (LiUNA) (emphasis added).

[677] Ontario's construction industry pushes for wearable COVID-19 tracing app.

[678] Trace me on my cellphone, July 6, 2020.

[679] Where is BC's COVID contact-tracing technology?

[680] Facedrive launches TraceSCAN Wearables pilot project in partnership with Labourers' International Union of North America (LiUNA).

[681] The governments of Canada and Quebec and the international community join forces to advance the responsible development of artificial intelligence.

[682] Ontario expanding data collection to help stop spread of COVID-19.

[683] Ontario opens up COVID-19 testing across the province.

[684] Ontario expanding data collection to help stop spread of COVID-19 (bracket added).

[685] Ontario appoints Special Advisor to develop health data platform.

[686] Ontario appoints Special Advisor to develop health data platform.

[687] Ontario appoints Special Advisor to develop health data platform.

[688] Ontario expanding data collection to help stop spread of COVID-19.

[689] Ontario expanding data collection to help stop spread of COVID-19.

[690] Download COVID Alert today.

[691] News Release: COVID Alert available for download beginning today - privacy-first, made-in-Ontario app notifies users of potential exposure to COVID-19.

[692] See e.g., Battling fast-moving COVID-19, Toronto's contact tracing system struggles to get up to speed.

[693] PM says a national contact tracing app is coming next month, how will it work? (bracket added).

[694] Canada has an army of volunteers ready to help fight COVID-19 – so why aren't we using them.

[695] Ontario Enhancing COVID-19 case and contact management (emphasis added).

[696] Ontario Enhancing COVID-19 case and contact management. See also: Lack of privacy oversight could hurt buy-in for COVID contact-tracing app, say critics.

[697] What is Salesforce?

[698]Salesforce – Update to our COVID-19 response.

[699]Salesforce – Update to our COVID-19 response.

[700] Salesforce – The State of Rhode Island is a trailblazer in testing and contact tracing efforts (emphasis added). See also: And the Littlest State Shall Lead the Way on Covid-19 (noting Gina Raimondo, the governor of Rhode Island, "realized that Salesforce's bread and butter — customer relationship management software — could be adapted easily to conduct significant contact tracing" and cold-called CEO Benioff, who sent a team, for free, to help Rhode Island build contact tracing software, which Salesforce then commercialized, in addition to launching Work.com, a platform that helps businesses and other institutions mitigate the spread of the virus when workplaces re-open).

[701] Salesforce – The State of Rhode Island is a trailblazer in testing and contact tracing efforts.

[702] Salesforce – The State of Rhode Island is a trailblazer in testing and contact tracing efforts (emphasis added).

[703] Salesforce – Update to our COVID-19 response.

[704] Privacy experts concerned about next stage of Ontario's reopening plan.

[705] Privacy experts concerned about next stage of Ontario's reopening plan. BC "has clearly spelled out that businesses should collect only first and last names, plus either a phone number or email address for one person among a party. B.C.'s rules also state the information should be kept for 30 days and is only to be used for contact tracing purposes." In contrast, Ontario urges businesses in specified sectors only to "consider operating by appointment and/or recording each patron's name and contact information for the purpose of contact tracing": Ibid.

[706] New Brunswick: New rules for collecting contact tracing info coming amid privacy concerns.

[707] New Brunswick: New rules for collecting contact tracing info coming amid privacy concerns.

[708] News Release: Ontario implementing additional measures at bars and restaurants to help limit the spread of COVID-19.
Measures to Further Protect the Health of Ontarians as the Province Continues to Re-open Under Stage 3 (citing Ontario government amended orders O. Reg 364/20: Rules for Areas in Stage 3 and O. Reg. 263/20: Rules for Areas in Stage 2, under the *Reopening Ontario (A Flexible Response to COVID-19) Act, 2020*). See also: Contact tracing information at Ontario bars, restaurants raises privacy concerns.

[709] Contact tracing information at Ontario bars, restaurants raises privacy concerns.

[710] Canadian health officials using Uber data to track COVID-19.

[711] Canadian health officials using Uber data to track COVID-19; Uber offers COVID-19 contact tracing help amid chaotic U.S. response,

[712] Canadian health officials using Uber data to track COVID-19 (bracket in original).

[713] As debate over contact tracing continues, CSE warns of foreign surveillance technology (emphasis added).

[714] As debate over contact tracing continues, CSE warns of foreign surveillance technology (emphasis added).

[715] Hard questions for policy-makers about digital contact tracing.

[716] More traditional methods of surveillance might be more valuable for contact-tracing than smartphone apps – and perhaps more intrusive ("So far, these tools have been greeted (thankfully) with more skepticism in Canada than in other societies.")

[717] Hard questions for policy-makers about digital contact tracing (bracket added).

[718] Hard questions for policy-makers about digital contact tracing.

[719] Hard questions for policy-makers about digital contact tracing ("Most importantly, Canada can learn from first-mover countries about how *not* to deploy digital contact tracing. It should not try to work out the technology options before it has answers to questions about policy options.")

[720] Hard questions for policy-makers about digital contact tracing.

[721] Hard questions for policy-makers about digital contact tracing.

[722] See e.g., "About Open Government", GoC, online: https://open.canada.ca/en/about-open-government (accessed 25 May 2020) (defining "Open Government" as "about making government more accessible to everyone" and citing the "Directive on Open Government", described as "Canada's 'open by default' policy, providing clear and mandatory requirements to departments which will ensure that Canadians get access [sic] the most government information and data possible.")

[723] Hard questions for policy-makers about digital contact tracing.

[724] Ethical guidelines for COVID-19 tracing apps.

[725] France offers a case study in the battle between privacy and coronavirus tracing apps (paragraph breaks deleted).

[726] One app per province? How Canada's federalism complicates digital contact tracing.

[727] The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System (brackets added).

[728] Bianca Wylie tweets, July 31-August 2, 2020.

[729] Bianca Wylie tweets, July 31-August 2, 2020.

[730] Who controls reins of Big Tech's COVID Alert app?

[731] Without early warning you can't have early response.

[732] Without early warning you can't have early response.

[733] The Logic, July 30, 2020.

[734] Without early warning you can't have early response.

[735] Hard questions for policy-makers about digital contact tracing.

[736] Does Covid-19 contact tracing pose a privacy risk? Your questions, answered.

[737] Coronavirus, invisible threats and preparing for resilience.

[738] Japan's new virus contact-tracing app promises privacy in bid for reach.

[739] The Challenge of Proximity Apps For COVID-19 Contact Tracing", Electronic Frontier Foundation.

[740] Bracelets, beacons, barcodes: wearables in the global response to COVID-19.

[741] Canada's privacy watchdogs see uptick in work amid pandemic.

[742] The Challenge of Proximity Apps For COVID-19 Contact Tracing", Electronic Frontier Foundation.

[743] European Union: COVID-19: protecting personal data – the new normal.

[744] See e.g., The Case For Contact Tracing Apps Built On Apple And Google's Exposure Notification System (arguing that "if 'completely free of privacy and security concerns' is the standard, then any form of contact tracing is impossible" and accusing privacy experts who identify privacy risks of decentralised Bluetooth apps – especially built on the Apple/Google API – as "rais(ing) specious problems" and "offer[ing] no solution other than privacy fundamentalism"). Historically, various "privacy segmentations" have divided consumer-citizens according to their privacy knowledge and preferences. Alan Westin's privacy segmentation, which was widely used in various fields and influenced US privacy law (e.g., "the predominant 'notice and choice' regime") and has been aptly criticized for its inaccurate description of privacy markets and consumer choices: divided the American public into three groups: "the privacy fundamentalists (high privacy concern and high distrust in government, business, and technology), the privacy pragmatists (mid-level concern and distrust), and the privacy unconcerned (no or low concern and distrust)": The privacy pragmatic as privacy vulnerable, p. 1.

[745] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 19.

[746] The security behind the NHS contact tracing app.

[747] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 20 (emphasis added).

[748] Implementing privacy by design, stressing it: "is a principle that many consider to be a, if not the, crucial element in protecting privacy rights meaningfully"; "has traditionally been regarded as the gold standard of privacy protection"; is "a marriage of two ideals: (i) protection of personal information; and (ii) its coinciding sustainable commercial use, centred around seven foundational principles" - "Principle 1 – Proactive not reactive: preventative not remedial. Principle 2 – Privacy as the default setting. Principle 3 – Privacy embedded into design. Principle 4 – Full functionality: positive-sum, not zero-sum. Principle 5 – End-to-end security: full lifecycle protection. Principle 6 – Visibility and transparency: keep it open. Principle 7 – Respect for user privacy: keep it user-centric").

[749] Implementing privacy by design. In November 2019, EDPB published its draft Guidelines 4/2019 on *Article 25: Data Protection by Design and by Default* ("DPbDD"), for public consultation until January 16, 2020. The guidelines "will form an important part of how privacy by design will be interpreted and implemented in Europe, with a downstream effect on any technology company who'll be supplying Data Controllers": Implementing privacy by design.

[750] Implementing privacy by design (emphasis added).

[751] "Privacy-first policy on DCTT" means, in the words of the World Economic Forum, that DCTT must "prioritize and protect privacy": COVID-19 contact tracing must be ethical and responsible. Here's why (emphasizing that "Though the overwhelming goal of the coming months will be to make progress against the global pandemic, it's essential that any contact tracing solution prioritize and protect individual privacy. We have the technology to do this; all that's needed is the will to implement it. Strong, clear standards around contact tracing that protect people's right to privacy as well as their health will be a major step in the right direction.").

[752] Privacy in the balance (citing Éloïse Gratton, a privacy and data protection lawyer at BLG).

[753] GDPR, a new privacy law, makes Europe world's leading tech watchdog.

[754] WHO: Contact tracing in the context of COVID-19 (Interim Guidance).

[755] WHO: Digital tools for COVID-19 contact tracing – Annex: contact tracing in the context of COVID-19 (Interim Guidance).

[756] Tracking and tracing COVID: protecting privacy and data while using apps and biometrics (bracket in original).

[757] EP & EC Joint European roadmap towards lifting COVID-19 containment measures.

[758] Joint statement on contact tracing, global scientists and researchers (citing European Parliament).

[759] EC Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection.

[760] Trace me on my cellphone, May 13, 2020 (citing EC statement, bracket added).

[761] EC: Mobile applications to support contact tracing in the EU's fight against COVID-19 - common EU toolbox for Member States.

[762] EC - Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures.

[763] EC - Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps (emphasis in original).

[764] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

[765] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

[766] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 48..

[767] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 4.

[768] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 49.

[769] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, paras. 14-16, 19 and 20 (emphasis in original) (noting "a large body of research has shown that *location data thought to be anonymised may in fact not be*, because "[m]obility traces of individuals are inherently highly correlated and unique" thus "can be vulnerable to re-identification attempts under certain circumstances").

[770] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 39.

[771] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 8.

[772] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 27.

[773] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, paras. 36-37.

[774] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 37.

[775] Implementing privacy by design (noting that under GDPR, the "controller" is the person who *determines* the means and processing of personal data).
[776] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 25.
[777] EC Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, para. 3.1.
[778] Trace me on my cellphone, May 14, 2020.
[779] EC: Interoperability guidelines for approved contact tracing mobile applications in the EU.
[780] EC - Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU (bracket added).
[781] Anonymization by decentralization? The case of COVID-19 contact tracing apps.
[782] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 42.
[783] COVID-19: when EU tracking apps meet the pandemic, trust and privacy by design are the hosts.
[784] EDPB statement on app interoperability.
[785] EDPB statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak.
[786] EDPB news release re: statement on the interoperability of contact tracing applications.
[787] Five key provisions a federal privacy law should include.
[788] Employer use of contact tracing apps: the good, the bad, and the regulatory.
[789] For text of bill, see: https://cdn.arstechnica.net/wp-content/uploads/2020/06/Exposure-Notification-Privacy-Bill-Text.pdf
[790] The US's draft law on contact tracing apps is a step behind Apple and Google; COVID-19 privacy protection bill introduced with bipartisan support.
[791] The US's draft law on contact tracing apps is a step behind Apple and Google.
[792] Republican senators to introduce the COVID-19 Consumer Data Protection Act.
[793] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 15.
[794] Data privacy laws collide with contact tracing efforts; privacy is prevailing.
[795] CNIL Opinion on the draft decree regarding the conditions for the implementation of the StopCovid app. This follows CNIL's April 2020 opinion on the app itself.
[796] France: CNIL approves of implementation of StopCovid app.
[797] France: CNIL approves of implementation of StopCovid app; France offers a case study in the battle between privacy and coronavirus tracing apps**;** The CNIL gives its opinion on the conditions for implementing the 'StopCovid' application.
[798] France: CNIL approves of implementation of StopCovid app; The CNIL gives its opinion on the conditions for implementing the 'StopCovid' application.
[799] Europe faces privacy concerns with contact-tracing apps.
[800] COVID-19 and contact-tracing apps in Canada.
[801] UK Government: Keeping workers and customers safe during COVID-19 in restaurants, pubs, bars and takeaway services: COVID-19 secure guidance for employers, employees and the self-employed; Businesses face privacy minefield over contact-tracing rules, say campaigners; UK's newly-opened pubs may face data protection nightmare.
[802] UK Government: Keeping workers and customers safe during COVID-19 in restaurants, pubs, bars and takeaway services: COVID-19 secure guidance for employers, employees and the self-employed, p. 1.
[803] Businesses face privacy minefield over contact-tracing rules, say campaigners (noting privacy experts warned about privacy risks, including personal data hoarding, loss, and misuse, for marketing or unwanted personal contact [e.g., stalking or harassment], which are particularly concerning in regard to minorities, women, and other vulnerable groups); UK's newly-opened pubs may face data protection nightmare (noting that due to the UK government's instruction, these businesses "will suddenly become data controllers for the first time – and subject to data protection rules under the EU's General Data Protection Regulation [GDPR]").
[804] Parliament of the Commonwealth of Australia, *Privacy Amendment (Public Health Contact Information) Act 2020*, No. 44, 2020, assented to May 15, 2020, online: https://www.legislation.gov.au/Details/C2020A00044.
[805] Criminal Lawyers' Association position on digital COVID-19 contact tracing; CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 15.
[806] Privacy commissioners: privacy laws not a barrier to effective COVID-19 response, emphasize compliance when using contact tracing apps (citing the Office of the Australian Information Commissioner).
[807] OPCC: Privacy review of the COVID Alert exposure notification application (citing Swiss Parliament, Loi fédérale sur la lutte contre les maladies transmissibles de l'homme [19 June 2020]).
[808] Ethical guidelines for COVID-19 tracing apps.
[809] Yes, Apple and Google have given us a serious contact tracing problem—here's why.
[810] Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.
[811] Coronavirus: how much does your boss need to know about you? (Ifeoma Ajunwa, assistant employment law professor at Cornell University in the US).
[812] Ethical guidelines for COVID-19 tracing apps.

[813] Anonymization by decentralization? The case of COVID-19 contact tracing apps.

[814] Joint statement on contact tracing, global scientists and researchers.

[815] https://exposurenotification.org/

[816] https://www.usdigitalresponse.org/

[817] TCN Coalition applauds Apple and Google's digital contact tracing announcement.

[818] https://exposurenotification.org/

[819] https://exposurenotification.org/

[820] CPE Race to trace: security and privacy of COVID-19 contact tracing apps, p. 15.

[821] Coronavirus statement.

[822] Coronavirus statement.

[823] Canadians' security and privacy must be protected in the race to trace.

[824] UPDATED: OPC now says it supports COVID-19 tracing app; FIPA Joint Statement to PM Trudeau on Covid Shield.

[825] CPE Race to trace: security and privacy of COVID-19 contact tracing apps.

[826] "Canadian privacy law" (aka "Canadian data protection law") means the Canadian legal framework for protecting personal information (see details below).

[827] Privacy and the COVID-19 outbreak, March 2020 (emphasis and bracket added)(referencing PT privacy and COVID-19 statements of Alberta, BC, Ontario, Newfoundland and Labrador, Quebec, Saskatchewan, Yukon, and NWT).

[828] Canada's federal privacy laws: background paper, p.1.

[829] See e.g., A typology of privacy (identifying "eight plus one primary types of privacy").

[830] See e.g., Supreme Court of Canada decision raises interesting issues about jurisdiction over privacy-impactful technologies.

[831] See e.g., Canada's federal privacy laws: background paper, p. 1 ("Privacy protection laws in Canada focus mainly on safeguarding personal information.")

[832] See e.g., Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 54 (noting personal information "is defined very broadly under Canadian Privacy Statutes as information about an identifiable individual").

[833] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 54. See also: *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, Paragraph 34.

[834] Expectations: OPC's guide to the privacy impact assessment process, March 2020.

[835] Brookings Report, Bridging the gaps: a path forward to federal privacy legislation, p. 32 (re: "precise" location data, online activities, metadata, noting these are included in certain US statutory definitions of "sensitive data"); Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps (re: photos, contact lists, "location information"); Expectations: OPC's guide to the privacy impact assessment process (re: personal opinions); and OPC a guide for individuals protecting your privacy (re: other listed items).

[836] Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps (referring to *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII), online: http://canlii.ca/t/1vxt3, accessed June 18, 2020) (paragraph breaks deleted).

[837] The privacy, data protection and cybersecurity law review - edition 6: Canada (citing PIPEDA Case Summary #2009-010 – Report of Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection).

[838] The privacy, data protection and cybersecurity law review - edition 6: Canada (citing Office of the Privacy Commissioner of Canada, 'Policy Position on Online Behavioural Advertising', 6 June 2012, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/).

[839] PIPEDA, subs. 2(1).

[840] See e.g., Modernizing Canada's Privacy Act ("Other countries have responded to these technological and societal changes with new laws to protect their citizens' personal information. These laws are sometimes called 'data protection' laws").

[841] A Data Privacy Day conversation with Canada's Privacy Commissioner.

[842] Part 1 of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), c 11.

[843] Modernizing Canada's Privacy Act.

[844] A typology of privacy, pp. 511-512 (brackets added).

[845] A typology of privacy, p. 153 and fn 93; OPC a guide for individuals protecting your privacy.

[846] OPC a guide for individuals protecting your privacy (noting "[t]he Supreme Court of Canada has stated that the Privacy Act has 'quasi-constitutional status', and that the values and rights set out in the Act are closely linked to those set out in the Constitution as being necessary to a free and democratic society.") See also Part 3.

[847] The GDPR, which came into force in May 2018, is a new privacy regime for all EU member states that imposes privacy protections for personal information *within and flowing out of* the EU. Other countries (e.g., Australia, New Zealand, and UK) have also changed their privacy law frameworks: Modernizing Canada's Privacy Act.

[848] COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic (bracket added).

[849] Brookings Report, Bridging the gaps: a path forward to federal privacy legislation, p. 27.

[850] Some PTs have privacy legislation that applies to municipalities: Modernizing Canada's Privacy Act.

[851] Public sector privacy legislation is federal (the *Privacy Act*) and PT. For details on the Privacy Act's application, see Appendix B.

[852] Private sector privacy legislation is federal (PIPEDA) and PT. For details on PIPEDA's application, see Appendix B.

[853] Health privacy legislation is PT only, and an example is Ontario's *Personal Health Information Protection Act,* 2004, S.O. 2004, c. 3, Sched. A ("PHIPA"), online: https://www.ontario.ca/laws/statute/04p03.

[854] Declaration of PHIPA as substantially similar to PIPEDA; Canada: Cybersecurity Comparative Guide (emphasis added) ("Under Section 26.2(b) of PIPEDA, if a province's legislation has been deemed substantially similar to Part 1 of PIPEDA, then the organisations to which provincial legislation applies may be exempt from the application of Part 1 in respect of the collection, use and disclosure of personal information *in that province*.")

[855] Canada: Cybersecurity Comparative Guide (citing these exemption orders: Organizations in the Province of Québec Exemption Order (SOR/2003-374); Organizations in the Province of British Columbia Exemption Order (SOR/2004-220); and Organizations in the Province of Alberta Exemption Order (SOR/2004-219)).

[856] Canada: Cybersecurity Comparative Guide.

[857] Declaration of PHIPA as substantially similar to PIPEDA. See also COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic (noting health information custodians include doctors, hospitals, and medical officers of health).

[858] Declaration of PHIPA as substantially similar to PIPEDA.

[859] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018 (noting the health privacy legislation of some PTs has been deemed substantially similar to PIPEDA and, as such, PIPEDA does not apply to businesses operating *within* those jurisdictions, other than federally-regulated businesses); Declaration of PHIPA as substantially similar to PIPEDA.

[860] Declaration of PHIPA as substantially similar to PIPEDA. PHIPA is deemed substantially similar and exempted from the application of Part 1 of PIPEDA by: Health Information Custodians in the Province of Ontario Exemption Order SOR/2005-399: Canada: Cybersecurity Comparative Guide (noting that other PTs with health-related privacy legislation that has been declared substantially similar to PIPEDA with respect to PHI are NB, Nfld + LD, and NS:

- New Brunswick: The Personal Health Information Privacy and Access Act (SNB 2009, c P-7.05) is deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in New Brunswick Exemption Order SOR/2011-265).
- Newfoundland and Labrador: The Personal Health Information Act (SNL 2008, c P-7.01) is deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, SI/2012-72.
- Nova Scotia: The Personal Health Information Act (SNS 2010, c 41) is deemed substantially similar and exempted from the application of Part 1 of PIPEDA by Personal Health Information Custodians in Nova Scotia Exemption Order SOR/2016-62.

[861] Ontario Privacy Laws for Lawyers ("It is important to note… that all personal information that is not personal health information will continue to be governed by PIPEDA").

[862] Canada: amendments to Ontario's health information legislation bring new obligations and penalties (noting that on March 25, 2020, "significant amendments" were made that bring new powers, obligations, and penalties, including: new powers for Ontario's privacy commissioner; higher penalties for offences; new duty to maintain electronic audit log; new concept of "consumer electronic service providers"; and ability to impose requirements related to information de-identification).

[863] For an overview of COVID-19 privacy guidance issued by *individual PT* privacy commissioners, see e.g., Privacy in a pandemic: privacy laws matter.

[864] A Data Privacy Day conversation with Canada's Privacy Commissioner (emphasizing that "[p]rivacy is much broader than data protection – although data protection seeks to participate in the protection of privacy").

[865] Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC.

[866] Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC.

[867] Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC.

[868] COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic.

[869] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018 (referencing PIPEDA and Alberta's PIPA).

[870] S.C. 1993, c. 38, online: https://laws.justice.gc.ca/eng/acts/T-3.4/

[871] PIAC response to procedural requests to dismiss May 2020 Part 1 Application.

[872] PIAC response to procedural requests to dismiss May 2020 Part 1 Application.

[873] May 2020 PIAC Part 1 Application Regarding Pandemic Contact Tracing.

[874] CRTC decision letter on May 2020 PIAC Part 1 Application on Contact Tracing.

[875] RSC, 1985, c. C-46, online: https://laws-lois.justice.gc.ca/eng/acts/c-46/.

[876] CQLR, c. C-12.

[877] CQLR, c. CCQ-1991.

[878] See e.g., COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic; Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018; Modernizing Canada's Privacy Act (noting privacy torts exist in some PTs and citing Section 5 of Quebec's Charter, which states "every person has a right to respect for his private life").

[879] Privacy in a pandemic: privacy laws matter. PIPEDA and Privacy Act exceptions are detailed in Part 3.

[880] Privacy in a pandemic: privacy laws matter. PIPEDA and Privacy Act exceptions are detailed in Part 3.

[881] S.C. 2005, c. 20, online: https://laws-lois.justice.gc.ca/eng/acts/q-1.1/page-1.html

[882] Finding our way through privacy, data gaps and pandemic response.

[883] R.S.O. 1990, c. H.7, online: https://www.ontario.ca/laws/statute/90h07.

[884] S-2.2, online: http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/S-2.2.

[885] Finding our way through privacy, data gaps and pandemic response.

[886] Privacy in a pandemic: privacy laws matter.

[887] Privacy in a pandemic: privacy laws matter (bracket added). For details on privacy commissioners' statements on privacy and COVID-19, see Part 3.

[888] May 2020 Joint OPCC-PT Privacy Commissioner COVID-19 Privacy Guidance (bracket added).

[889] The rise of the digital robber barons.

[890] Privacy in a pandemic: privacy laws matter.

[891] Canada extends mandatory requirements under the Quarantine Act for anyone entering Canada.

[892] Privacy in a pandemic: privacy laws matter; Criminal Lawyers' Association position on digital COVID-19 contact tracing. BC's Minister of Citizens' Services enacted Ministerial Order No. MO85 (directly dealing with the province's public sector privacy law and carving out new exceptions explicitly authorizing PHAs to disclose personal information within and outside Canada, including using third party tools and applications, until June 30, 2020, if certain conditions are met) and on March 13, 2020, the Quebec government declared a state of health emergency (which permits PHAs to gain access to personal data in order to protect the health of the population: Privacy in a pandemic: privacy laws matter. On March 17, 2020, Ontario declared an emergency pursuant to Order in Council 518/2020 (Ontario Regulation 50/20), pursuant to the *Emergency Management and Civil Protection Act.*

[893] Ontario extends declaration of emergency until July 24, 2020.

[894] Ontario extends Emergency Orders to July 29, 2020. A full list of emergency orders (including the Declaration of Emergency) can be found at https://www.ontario.ca/page/emergency-information?_ga=2.126217357.1486010611.1593459562-897347386.1591403205

[895] Tweet by reporter Mike Crawley re extension of Ontario's state of emergency (citing Solicitor General Sylvia Jones) (paragraph break deleted).

[896] *O. Reg. 120/20: ORDER UNDER SUBSECTION 7.0.2 (4) OF THE ACT - ACCESS TO COVID-19 STATUS INFORMATION BY SPECIFIED PERSONS filed April 3, 2020 under Emergency Management and Civil Protection Act, R.S.O. 1990, c. E.9.*

[897] Criminal Lawyers' Association position on digital COVID-19 contact tracing. CLA maintains that emergency sub-orders like this "do not authorize sharing of *digital contact tracing information* with law enforcement" because it goes beyond simply infection status: Ibid (emphasis added).

[898] *O. Reg. 190/20: ORDER UNDER UNDER SUBSECTION 7.0.2 (4) OF THE ACT - ACCESS TO PERSONAL HEALTH INFORMATION BY MEANS OF THE ELECTRONIC HEALTH RECORD*, online: https://www.ontario.ca/laws/regulation/200190.

[899]Emergency information: provincial status on COVID-19, update on July 31 (paragraph breaks deleted).

[900]Emergency information: provincial status on COVID-19, update on July 31 (paragraph breaks deleted).

[901] Ontario Government agrees to human rights groups' demands to end police access to COVID database (referencing Notice of Application for judicial review of O. Reg 120/20 filed with Ontario Superior Court of Justice (Division Court) by CCLA et al on July 7, 2020). In light of the revocation, the human rights groups decided to end the litigation: Ibid.

[902] Privacy in a pandemic: privacy laws matter.

[903] Privacy in a pandemic: privacy laws matter (providing the following list, plus a brief summary of each PT guidance, and noting "[w]e were unable to locate similar guidance applicable to organizations in Nunavut and Prince Edward Island").

[904] Ontario OIPC: Impact of COVID-19.

[905] Alberta OIPC: Privacy in a pandemic.

[906] BC Privacy Commissioner's statement on COVID-19.

[907] "Longer extensions under FIPPA: advisory for public bodies about extensions under FIPPA during the COVID-19 pandemic", undated, online: https://www.ombudsman.mb.ca/info/longer-extensions-under-fippa.html

[908] NB Privacy Commissioner Guidance: privacy in emergency situations.

[909] NL + LD Privacy Commissioner: Don't blame privacy (which is "intended to shine some light on where the communication line is when privacy and urgent circumstance collide. The goal is to demonstrate how to not unnecessarily violate privacy, while also preventing unwarranted concerns from slowing response times.")

[910] NWT OIPC: Privacy in a pandemic.

[911] Nova Scotia Privacy Commissioner's statement on COVID-19.

[912] QC Privacy Commissioner – COVID-19: Protection des renseignements personnels et sécurité de l'information.

[913] Updated Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on COVID-19.

[914] Actions being taken by Yukon Ombudsman, Information and Privacy Commissioner and Public Interest Disclosure Commissioner in response to COVID-19 - Updated March 18 2020.

[915] Canada, U.S. attorneys general discussed law to speed up police access to data across borders.

[916] Canada, U.S. attorneys general discussed law to speed up police access to data across borders.

[917] Canada, U.S. attorneys general discussed law to speed up police access to data across borders.

[918] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act.

[919] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act (noting PHAC is akin to the US Centers for Disease Control and Prevention ["CDC"]); Health Portfolio; Canadian Network for Public Health Intelligence.

[920] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act.

[921] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act.

[922] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act.

[923] Canada's lost months: When COVID-19's first wave hit, governments and health officials were scattered and slow to act (emphasis added).

[924] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[925] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[926] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[927] See e.g., PIPEDA s. 10.1 (1) ("An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.")

[928] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55 (referencing PIPEDA and Alberta's PIPA).

[929] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[930] PIPEDA principle 4.3.4 ("The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information [for example, medical records and income records] is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.").

[931] See PIPEDA principle 4.3.4 (above) as well as 4.3.6, 4.7, 4.7.2 and 4.9.1. There is significant OPCC guidance and findings on sensitivity in various contexts, and health is always sensitive.

[932] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[933] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, pp. 55-56.

[934] Health data requires explicit consent except for very rare exceptions, notably the exception for telling someone their relative is in hospital in PIPEDA s. 7.

[935] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55..

[936] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55.

[937] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, pp. 55-66.

[938] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018 , p. 56.

[939] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, pp. 56, 58.

[940] No particular title is required, however common titles include Chief Privacy Officer or Privacy Officer: Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 57.

[941] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, pp. 56, 61.

[942] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[943] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018 (referencing PIPEDA and Alberta's PIPA). Pending the outcomes of ongoing FPT privacy legislation reform efforts, new individual rights could be introduced (see details below).

[944] Brookings Report, Bridging the gaps: a path forward to federal privacy legislation, p. 63.

[945] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[946] Exceptions vary across statutes (e.g., data subject to solicitor-client or litigation privilege; confidential commercial information; information about another individual, information related to national security, and information from a formal dispute resolution process): Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[947] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[948] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, .p. 56.

[949] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[950] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[951] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[952] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, pp. 56, 58.

[953] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 56.

[954] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 57.

[955] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 57.

[956] Statistics Canada, privacy impact assessment.

[957] TBS Directive on privacy impact assessment.

[958] Finding our way through privacy, data gaps and pandemic response.

[959] Interim directive on Privacy Impact Assessment.

[960] Finding our way through privacy, data gaps and pandemic response.

[961] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 61.

[962] Workplace privacy, an increasingly important issue in the Information Age.

[963] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 61.

[964] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 61.

[965] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018 (underline added).

[966] OPCC Annual Report.

[967] Canada's out-of-date online privacy rules aren't protecting you.

[968] Who controls reins of Big Tech's COVID Alert app?

[969] A Data Privacy Day conversation with Canada's Privacy Commissioner.

[970] OPCC Annual Report.

[971] A Data Privacy Day conversation with Canada's Privacy Commissioner.

[972] Shrems II: the saga continues, explaining that: "Under EU law, an organization may only transfer 'personal data' about an individual to a non-EU country for processing if the destination country 'ensures an adequate level of protection'. The European Commission has the authority to make a determination of whether the protections afforded to personal data in a given third country are or are not 'adequate' in this regard. In some cases 'adequacy' decisions apply broadly. In the case of Canada, for example, the European Commission concluded that Canada's PIPEDA is sufficiently similar to European laws that they were inherently adequate." (paragraph breaks deleted).

[973] No longer fit for purpose: why Canadian privacy law needs an update.

[974] Discussion paper: Ontario private sector privacy reform.

[975] A Data Privacy Day conversation with Canada's Privacy Commissioner (bracket added).

[976] Canada's Digital Charter: trust in a digital world.

[977] Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches.

[978] Canada's Digital Charter: Trust in a digital world.

[979] Modernizing Canada's Privacy Act.

[980] Strengthening privacy for the digital age: proposals to modernize the Personal Information Protection and Electronic Documents Act.

[981] Fifth update report on developments in data protection law in Canada: Report to the European Commission June 2019.

[982] December 2019 ISI Minister mandate letter; December 2019 Heritage Minister mandate letter.

[983] Telecom in the spotlight in new Bains mandate letter (citing letter).

[984] Modernizing Canada's Privacy Act (bracket added).

[985] Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches. See also: Privacy Penalties – Canadian Competition Bureau wades into privacy enforcement ("the current focus of all governments on COVID-19 means that substantive changes to PIPEDA will likely have to wait") and Ontario launches consultation on new private sector data protection law ("The COVID-19 crisis appears to have derailed [once again] the introduction of a bill to amend PIPEDA and it is not clear when such a bill will be introduced"). Previously, ISI Minister Bains said GoC might bring forward a revised PIPEDA in fall 2020: Data wars: why technology advocates believe privacy regulations need serious reform.

[986] Pandemic has increased the need for privacy rights, OPC told Guilbeault (citing letter).

[987] A Data Privacy Day conversation with Canada's Privacy Commissioner; OPCC Annual Report.

[988] OPCC Annual Report.

[989] Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC.

[990] Canada: modernizing federal privacy laws: suggested approaches of the federal government and the OPC (bracket added).

[991] Pandemic has increased the need for privacy rights, OPC told Guilbeault.

[992] Pandemic has increased the need for privacy rights, OPC told Guilbeault.

[993] News Release: Conservatives request Privacy Commissioner investigate federal contact tracing app and ArriveCAN app (citing Privacy Commissioner Therrien).

[994] Outdated privacy laws may hamper COVID-19 tracing: Therrien.

[995] Outdated privacy laws may hamper COVID-19 tracing: Therrien.

[996] Privacy in the balance (citing Scassa).

[997] Outdated privacy laws may hamper COVID-19 tracing: Therrien.

[998] News Release: Conservatives request Privacy Commissioner investigate federal contact tracing app and ArriveCAN app.

[999] Published May 7, 2020, online: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

[1000] Published April 27, 2020, online: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/

[1001] Published March 2020, online: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/

[1002] TLDR; 15 Excerpts from the Privacy Commissioner's Review of Health Canada's COVID 19 Contact Tracing App.

[1003] News release: Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness (paragraph breaks deleted).

[1004] OPCC: Privacy review of the COVID Alert exposure notification application.

[1005] OPCC: Privacy review of the COVID Alert exposure notification application (citing "*Privacy Act* Modernization: A discussion Paper. Greater certainty for Canadians and government: delineating the contours of the *Privacy Act* and defining important concepts", p. 4).

[1006] OPCC: Privacy review of the COVID Alert exposure notification application ("For instance, while de-identified information might be exempted from certain provisions of the Privacy Act, or their application nuanced, other provisions would continue to apply; de-identified information should not be completely carved out").

[1007] Canada: privacy protection in Quebec: an overview of amendments to the law governing the private sector

[1008] Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches,

[1009] Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches.

[1010] Canada: Quebec introduces new amendments to its privacy regimes. See also: Canada: privacy protection in Quebec: an overview of amendments to the law governing the private sector.

[1011] Jennifer Stoddart: Quebec takes the lead in privacy law but overreaches.

[1012] News release: Ontario launches consultations to strengthen privacy protections of personal data (specifying the consultation includes an online survey, written submissions, and "web conferences"); Discussion paper: Ontario private sector privacy reform.

[1013] News release: Ontario launches consultations to strengthen privacy protections of personal data; Discussion paper: Ontario private sector privacy reform.

[1014] Supreme Court of Canada decision raises interesting issues about jurisdiction over privacy-impactful technologies.

[1015] EU-US Privacy Shield invalid: Schrems II.

[1016] Shrems II: the saga continues. In particular, CJEU invalidated the EC decision that the EU-US Privacy Shield is "adequate" for transferring personal data to the US and, in "a double whammy", also ruled that transferring personal data to the US pursuant to EC-adopted standard data protection clauses could also be found invalid by local data protection authorities: EU-US Privacy Shield invalid: Schrems II.

[1017] EU ruling on US agreement may nudge Canada to update our privacy law: Cavoukian, Jul 17, 2020, IT World Canada.

[1018] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1019] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1020] OPCC: Privacy review of the COVID Alert exposure notification application.

[1021] OPCC: Privacy review of the COVID Alert exposure notification application (emphasis added).

[1022] Regarding implementation and operational stages and court references, see e.g., Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1023] Criminal Lawyers' Association position on digital COVID-19 contact tracing. Some PT privacy commissioners have power to conduct audits, whereas other do not.

[1024] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1025] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1026] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1027] Coronavirus statement.

[1028] Plans for single COVID-19 contact tracing app facing resistance: health minister.

[1029] Federal, provincial watchdogs still waiting for full privacy assessment on national contact-tracing app.

[1030] Federal, provincial watchdogs still waiting for full privacy assessment on national contact-tracing app.

[1031] Criminal Lawyers' Association position on digital COVID-19 contact tracing.

[1032] To protect our privacy rights, COVID-19 surveillance measures need a squeaky wheel.

[1033] To protect our privacy rights, COVID-19 surveillance measures need a squeaky wheel (paragraph breaks deleted).

[1034] France approves release of controversial COVID-19 tracking app (citing Nojeim).

[1035] A new data governance model for contact tracing: authorized public purpose access. See also Contact tracing and privacy: we need both to restart the economy and get employees back to work (arguing "the solution to increasing contact tracing app adoption rates in the absence of a mandated model" could be replacing "over reliance on a voluntary, consent model for using citizen data" with an enhanced "accountability framework").

[1036] No longer fit for purpose: why Canadian privacy law needs an update.

[1037] Expectations: OPC's guide to the privacy impact assessment process, March 2020 (bracket added, reflecting separate statement that "[a]n effective PIA can help build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices").

[1038] OPC a guide for individuals protecting your privacy; COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic.

[1039] OPCC summary of privacy laws in Canada; OPC a guide for individuals protecting your privacy.

[1040] Modernizing Canada's Privacy Act.

[1041] Alberta's *Personal Information Protection Act*, S.A. 2003, ch. P-6.5 ("PIPA Alberta").

[1042] British Columbia's *Personal Information Protection* Act, S.B.C. 2003, ch. 63 ("PIPA BC").

[1043] Québec's *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., ch. P-39.1 ("Québec Privacy Act").

[1044] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 54.

[1045] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018.

[1046] OPC a guide for individuals protecting your privacy (paragraph breaks deleted).

[1047] Modernizing Canada's Privacy Act: what we heard report – summer and fall 2019 (noting "[t]here was broad support for adding privacy principles", including from "government institutions").

[1048] OPC a guide for individuals protecting your privacy.

[1049] Access to information that is *not* personal information must be made under the separate *Access to Information Act*, which is enforced by the Office of the Information Commissioner of Canada: OPC a guide for individuals protecting your privacy.

[1050] Canada's federal privacy laws: background paper (brackets added); March 2020 OPCC COVID-19 Privacy Guidance.

[1051]March 2020 OPCC COVID-19 Privacy Guidance.

[1052] Canada's federal privacy laws: background paper (brackets and emphasis added).

[1053] OPC a guide for individuals protecting your privacy (updated December 2015). OPCC periodically updates its overview of the PIPEDA fair information principles. See e.g.: PIPEDA fair information principles (revised May 2019).

[1054] OPC a guide for individuals protecting your privacy.

[1055] Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps.

[1056] Top ten dos and don'ts for privacy impact assessments. This is a "quick reference document" for preparing PIAs *for federal government institutions,* and it expressly directs readers to the mobile app guidance document ("Our Office has produced guidance documents addressing various privacy issues, such as biometrics, cloud computing, mobile apps, and covert and overt video surveillance, which may help you throughout the PIA process.") However, the guidance states it "is intended for the private sector" and that "developers who may also be building apps for governments, public bodies or health custodians should be aware of, and able to comply with, other privacy laws across Canada": Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps.

[1057] Joint OPCC and Alberta and BC Privacy Commissioner 2012 Guidance on Mobile Apps (brackets added, bold in original).

[1058] Joint OPCC and Alberta and BC Privacy Commissioner 2018 Guidance on Meaningful Consent.

[1059] Privacy watchdogs taking a look at Tim Hortons app's location tracking technology (brackets added).

[1060] Privacy watchdogs taking a look at Tim Hortons app's location tracking technology (brackets added).

[1061] Tim Hortons scaling back data collection as four privacy watchdogs announce joint investigation into app (explaining that investigative journalism discovered the app "was accessing a user's location data as often as every three to five minutes, even when the app wasn't open. That data was being transmitted to an American company called Radar Labs, which was analyzing the data to infer where users lived and worked, and the app logged every time the company thought a user was visiting one of Tim Hortons' competitors, such as Starbucks or McDonald's" and noting that subsequently the company said it has discontinued the app's *background* data collection practices); Privacy watchdogs taking a look at Tim Hortons app's location tracking technology; Double-double tracking: how Tim Hortons knows where you sleep, work and vacation;

[1062] Privacy watchdogs taking a look at Tim Hortons app's location tracking technology.

[1063] Tim Hortons scaling back data collection as four privacy watchdogs announce joint investigation into app (citing Brenda McPhail, director of the Privacy, Surveillance, and Technology Project with the Canadian Civil Liberties Association).

[1064] Tim Hortons facing class-action lawsuit over app location tracking.

[1065] See e.g., PIPEDA s. 10.1 (1) ("An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.")

[1066] Chapter 7: Canada, in The International Comparative Guide to Data Protection 2018, p. 55 (referencing PIPEDA and Alberta's PIPA).

[1067] PIPEDA, *Breach of Security Safeguards Regulations*.

[1068] A full year of mandatory data breach reporting: what we've learned and what businesses need to know (emphasis in original) (noting that previously, reporting to OPCC was voluntary); OPC releases mandatory breach reporting guidance (noting "significant harm" includes "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property" and "'real risk of significant harm' must be determined based on an assessment of the sensitivity of the personal information involved in the breach and the probability the personal information have been/is/will be misused.")

[1069] See e.g., OPCC Mandatory Breach Reporting Guidance.

[1070] Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps (citing FPT privacy commissioners' joint statement and Privacy Commissioner of Canada's statement).

[1071] COVID-19 and contact-tracing apps in Canada.

[1072] COVID-19 impact: Canada's privacy commissioners outline guidance for governments and developers of contact tracing technology (bracket and emphasis added).

[1073] May 2020 Joint OPCC-PT Privacy Commissioner Guidance; Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps; COVID-19 and contact-tracing apps in Canada; COVID-19 and contact-tracing apps in Canada; COVID-19 impact: Canada's privacy commissioners outline guidance for governments and developers of contact tracing technology (bracket and emphasis added); Privacy commissioners: privacy laws not a barrier to effective COVID-19 response, emphasize compliance when using contact tracing apps.

[1074]COVID-19 impact: Canada's privacy commissioners outline guidance for governments and developers of contact tracing technology.

[1075] Privacy commissioners: privacy laws not a barrier to effective COVID-19 response, emphasize compliance when using contact tracing apps.

[1076] Federal, provincial watchdogs still waiting for full privacy assessment on national contact-tracing app.

[1077] COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives ("(w)hile this particular framework is targeted at government institutions, it includes some references to private-sector organizations and how these principles are equally applicable"); Canadian data privacy regulator releases guidance for Canadian privacy law compliance during COVID-19 ("While the April 2020 compliance framework is primarily intended to guide government agencies in compliance with the Privacy Act, a majority of these principles apply to private entities struggling with PIPEDA compliance.")

[1078] April 2020 OPCC Guidance.

[1079] April 2020 OPCC Guidance.

[1080] April 2020 OPCC Guidance; COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives; Canadian data privacy regulator releases guidance for Canadian privacy law compliance during COVID-19.

[1081] April 2020 OPCC Privacy Guidance.

[1082] COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives.

[1083] COVID-19 and contact-tracing apps in Canada (stating the April 2020 OPCC Guidance "set(s) out the same principles as (the May 2020 Joint OPCC-PT Privacy Commissioner Guidance) to guide the government in the assessment of measures proposed to combat COVID-19 and that have an impact on the privacy of Canadians. It is these same principles that form the backbone of the federal privacy legislation and provincial privacy legislation").

[1084] Outdated privacy laws may hamper COVID-19 tracing: Therrien (bracket added).

[1085] A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 (aka April 2020 OPCC COVID-19 Privacy Guidance).

[1086] COVID-19 and privacy: federal Privacy Commissioner publishes framework to help government institutions assess privacy-impactful initiatives.

[1087] A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 (aka April 2020 OPCC COVID-19 Privacy Guidance).

[1088] March 2020 OPCC Guidance; Canadian data privacy regulator releases guidance for Canadian privacy law compliance during COVID-19; OPC issues guidance on federal privacy laws in light of the COVID-19 outbreak.

[1089] March 2020 Guidance.

[1090] OPC issues guidance on federal privacy laws in light of the COVID-19 outbreak.

[1091] March 2020 Guidance. See also OPC issues guidance on federal privacy laws in light of the COVID-19 outbreak.