In the matter of

Part 1 Application submitted by PIAC regarding COVID-19 exposure notification applications – Scope of issues to be considered by the Commission in the context of this Part 1 application

Comments of

Canadian Wireless Telecommunications Association

November 27, 2020

INTRODUCTION

1. The Canadian Wireless Telecommunications Association ("CWTA") is the recognized authority on wireless issues, developments and trends in Canada. Its membership is comprised of companies that provide services and products across the wireless industry, including wireless carriers and manufacturers of wireless equipment. This submission is made on behalf of CWTA's telecommunication service provider members ("TSPs"). To the extent that there is any inconsistency between CWTA's submission and that of a CWTA member in this proceeding, in regards to the position of such CWTA member, the member's submission shall prevail.

2. CWTA is in receipt of a Part 1 Application filed by the Public Interest Advocacy Centre ("PIAC") dated 9 September 2020 (the "Application") [1] and the Canadian Radio-television and Telecommunication Commission's (the "Commission") process letter dated 28 October 2020 in relation to the Application (the "October 2020 Letter").

3. The Application represents PIAC's second attempt to launch a proceeding before the Commission into PIAC's unsubstantiated concerns regarding the use of personal information by various levels of government in the roll-out of COVID-19 exposure notification mobile applications (specifically the COVID Alert and ABTraceTogether applications) (together, the "COVID-19 Apps") and the alleged potential involvement by TSPs in the operation of these apps.

4. Federal, provincial and territorial privacy regulators have thoroughly reviewed and continue to provide extensive oversight of the COVID-19 Apps. For example, the COVID Alert App was developed in consultation with privacy commissioners and in accordance with the privacy principles expressed by these commissioners in a May 2020 Joint Statement.[2] In addition, the Office of the Privacy Commissioner of Canada ("OPC"), the Information and Privacy Commissioner of Ontario, the Information and Privacy Commissioner of Newfoundland and Labrador, and the Office of the Information and Privacy Commissioner of Alberta have deemed the COVID-19 Apps to be privacy-sensitive.[3] In particular, the OPC confirmed that the design of the COVID Alert app meets all of the privacy principles outlined in the May 2020 Joint

---

[1] Public Interest Advocacy Centre, *Part 1 Application Regarding "COVID Alert" App, "ABTraceTogether" App and Related Matters*, 9 September 2020 ("PIAC Application").

[2] Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, 7 May 2020, https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

[3] See Office of the Privacy Commissioner of Canada ("OPC"), *Privacy review of the COVID Alert exposure notification application,* 31 July 2020, https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/ ("Review of the COVID Alert App"); Information and Privacy Commissioner of Ontario, *Re. IPC Recommendation to the Government of Ontario regarding COVID Alert,* 30 July 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; Information and Privacy Commissioner of Newfoundland and Labrador, 3 September 2020, https://www.gov.nl.ca/releases/2020/oipc/0903n04-2/; and Office of the Information and Privacy Commissioner of Alberta, *ABTraceTogether Privacy Impact Assessment Review Report,* July 2020, https://www.oipc.ab.ca/media/1089098/Report_ABTraceTogether_PIA_Review_Jun2020.pdf.

Statement.[4] The OPC was also satisfied that the COVID Alert App includes very significant privacy protections and noted that the federal government has committed not to use the data it collects from the COVID Alert App to identify or attempt to identify users unless for security purposes or when required by law.[5]

5. In addressing PIAC's first application filed earlier this year in May, the Commission stated in a letter dated 17 August 2020 that PIAC's privacy concerns and claims regarding TSPs' participation in contact tracing applications were unsubstantiated.[6] Nevertheless, through this second application, PIAC continues to insist – unnecessarily – that the Commission inquire into the federal and provincial governments' collection and use of personal information in relation to the COVID-19 Apps and the potential for alleged TSP involvement in such collection and use.

6. In the October 2020 Letter, the Commission has appropriately limited the scope of its consideration of the Application to "matters subject to the Act," namely: (1) issues that pertain to the role of TSPs in handling of confidential information; (2) issues relating to what information should qualify as confidential customer information ("CCI"); and (3) any resulting measures that should apply to the TSP's collection, use and disclosure of that information.[7]

7. Within the above-noted context, CWTA respectfully submits that PIAC's COVID-app disclosure request ("CADR") proposal is a solution in search of a problem – one that would, if adopted, impose an entirely unnecessary additional layer of privacy regulation. More specifically, as discussed in further detail below, there is simply no need for the measures proposed by PIAC given that:

   (a) TSPs are not involved in the development, implementation or operation of exposure notification applications, including the COVID-19 Apps, which have been thoroughly reviewed and vetted by federal and provincial privacy commissioners. To the extent that there are any privacy concerns with the COVID-19 Apps, or how the government could hypothetically misappropriate and misuse data collected from the apps, these concerns should be raised with the respective government authorities that operate the apps and/or with the applicable privacy commissioners;

   (b) To CWTA's knowledge, none of its members have received any requests from government or law enforcement authorities for subscriber information in relation to the COVID-19 apps, nor do they expect to receive any such requests based on the government's representations that it will not attempt to identify users of the apps.

[4] OPC, Review of the COVID Alert App.
[5] OPC, Review of the COVID Alert App.
[6] Telecom – Commission letter addressed to John Lawford (Public Interest Advocacy Centre), *Re. Application submitted by the Public Interest Advocacy Centre regarding pandemic contact-tracing by major Canadian telecommunications service providers*, 17 August 2020 ("Commission's August 2020 Letter").
[7] Telecom – Commission Letter addressed to the Distribution list and Interested Persons, *Re: Part 1 application submitted by PIAC regarding COVID-19 exposure notification applications – Scope of issues to be considered by the Commission in the context of this Part 1 application,* 28 October 2020 ("Commission's October 2020 Letter").

Quite simply, the apps do not require subscriber information from CWTA members in order to function;

(c) Hypothetically, were government or law enforcement authorities to request subscriber information from a TSP member in connection with the COVID-19 Apps (or otherwise), the TSP would respond in accordance with the highly developed legal framework set out in applicable laws of general application, including the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[8] the *Criminal Code*[9] and the *Canadian Security Intelligence Service Act* ("*CSIS Act"*)[10]. CWTA's TSP members will only disclose subscriber personal information to government or law enforcement authorities that request the information, without the knowledge and consent of the subscriber, under limited circumstances prescribed by law and in accordance with that law. Contrary to PIAC's allegations, under no circumstances would a member disclose a subscriber's personal information to a government or law enforcement authority pursuant to a "simple request" in connection with the COVID-19 Apps;

(d) Without in any way conceding the point that TSPs are not involved in the operation of the COVID-19 Apps, taken together, the well-developed PIPEDA framework and the Commission's CCI framework adequately address the handling of personal information by TSPs. Contrary to PIAC's understanding, CCI is broadly defined to include all subscriber information held by TSPs, including WSPs and resellers, other than the customer's name, address and a listed telephone number. This would include, for example, a subscriber's IP address information and transmission data. As such, there is no need to re-open the Commission's CCI framework.

A. TSPS DO NOT HAVE ANY ROLE IN THE OPERATION OF THE COVID-19 APPS

8. The fundamental flaw in the PIAC Application is that there are no facts and no actual issues that give rise to an exercise of the Commission's jurisdiction. Instead, the Application rests on an entirely speculative foundation that TSPs could somehow be drawn into privacy breaches by government actors from the mere fact that the COVID-19 Apps, like all other applications, use telecommunications networks.[11] PIAC goes so far as to insinuate that new facts reveal the "role" of TSPs in privacy violations in relation to the operation of the COVID-19 Apps.[12] This is patently untrue. No evidence of such privacy violations have been provided by PIAC in support of this unfounded allegation.

9. CWTA and its TSP members do not play any role in the operation of the COVID-19 Apps, let alone engage in any privacy violations in connection with them.

[8] S.C. 2000, c.5 ("PIPEDA").
[9] R.S.C., 1985, c. C-46 ("*Criminal Code*").
[10] R.S.C., 1985, c. C-23.
[11] PIAC Application, paragraph 35.
[12] PIAC Application, paragraphs 4 and 35.

10. As the Commission already confirmed in its letter dated 17 August 2020 in response to PIAC's initial application filed with the Commission on 4 May 2020, TSPs are not involved in the development, implementation or operation of contact tracing applications.[13] The factual circumstances informing the Commission's determinations have not changed since August 2020. PIAC has not provided any evidence to the contrary.

11. The COVID-19 Apps were developed and are operated by various levels of government, health authorities and third-party developers. TSPs do not collect or record any information from the apps nor are they involved in the matching or notification of any positive diagnoses. TSPs provide subscribers with the networks over which mobile applications, such as the COVID-19 Apps, operate. The role that TSPs have in the transmission of data associated with the COVID-19 Apps is the same as data associated with any and all other third-party mobile applications.

12. As such, PIAC's Application invites the Commission to make binding determinations in the absence of any factual evidence that a problem needing redress exists. The Commission should not allow itself to be drawn into making determinations based on pure conjecture and speculation.

B. TSPS THOROUGHLY REVIEW AND ASSESS EACH REQUEST FROM A GOVERNMENT OR LAW ENFORCEMENT AUTHORITY

13. Notwithstanding the detailed reviews of the COVID-19 Apps conducted by privacy commissioners, PIAC appears to continue to harbour privacy-related reservations regarding the operation of these applications. Given this, CWTA respectfully submits that PIAC should raise its concerns with government authorities that operate the apps and/or with the privacy commissioners that reviewed the apps, not with TSPs that merely facilitate the transmission of app data over their networks.

14. That being said, CWTA wishes to dispel the misinformation propagated by PIAC's Application that TSPs provide government and law enforcement authorities with subscriber information pursuant to "simple requests."[14] That is not how Canadian TSPs operate.

15. In connection with the COVID-19 Apps, CWTA members will not disclose subscriber information to government or law enforcement authorities upon a "simple request". PIAC is incorrect in this assertion and offers no concrete evidence to support this unjustified allegation.

16. In addition to rules established by the Commission, all TSPs are subject to the comprehensive privacy framework established by PIPEDA, including the rules for how personal information is disclosed to government and law enforcement authorities without an individual's knowledge and consent.

[13] Commission's August 2020 Letter.
[14] PIAC Application, paragraphs 31 and 37.

17. Specifically, member TSPs will only disclose subscriber information to a government or law enforcement authority when presented with a valid order made by a court, person or body with the jurisdiction to compel the information (e.g., a production order or warrant) or where the authority has identified its lawful authority to obtain the information.

18. Despite PIAC's claims, every request by a government or law enforcement authority for the disclosure of subscriber personal information is thoroughly reviewed by CWTA's member TSPs before they respond to the request. These TSPs have developed comprehensive lawful access policies, in accordance with case law, such as *R. v. Spencer*,[15] and other legal precedents, that govern when and under what circumstances the TSP will respond to a request for subscriber information from a government or law enforcement authority, none of which permit careless disclosure. TSPs have trained professionals that review and assess all requests and consult with their Chief Privacy Officers and internal or external privacy counsel if there are any issues, concerns or questions related to a request.

19. In all instances, member TSPs will not disclose subscriber personal information to a government or law enforcement authority unless pre-defined procedures and conditions are met. First and foremost, members will review the validity of each request and verify the requestor's lawful authority. Members will also review requests for appropriate jurisdiction, mistakes, errors or omissions and the breadth and scope of the request. TSPs routinely ask for additional information and justification from authorities, push back against incomplete, incorrect or overly broad requests and require any errors to be remedied before fulfilling a request.

20. CWTA's members have a history of challenging lawful access requests, including in the courts, to protect and assert the privacy interests of subscribers.[16] In one notable challenge brought to court by Rogers and TELUS, the TSPs successfully challenged a broad "tower dump"[17] production order obtained by Peel Regional Police that was held to have infringed section 8 of the *Canadian Charter of Rights and Freedom*.[18] As PIAC's own Executive Director and General Counsel John Lawford recognized, Rogers and TELUS' successful challenge was a win for privacy advocates and subscribers: "It's a good decision … Probably about the best one you could get considering it may actually result in some changes in practice."[19]

21. TSPs apply these same principles and practices to the interpretation and application of their obligations under the CRTC's CCI rules. To be clear, there are no "gaps" between privacy laws

[15] 2014 SCC 43.
[16] See *R v. Rogers Communications,* 2016 ONSC 70 ("*R v. Rogers Communications*"); *R v. TELUS Communications Co.,* 2015 ONSC 3964; and *R v. TELUS Communications Co.,* 2013 SCC 16.
[17] A "tower dump" production order is an order for all records of cellular traffic through a particular cell tower over a specified time period.
[18] *R v. Rogers Communications,* paragraph 43.
[19] Robin Levinson King, "Peel police violated cellphone customers' charter rights, judge rules," *The Star*, January 14, 2016, https://www.thestar.com/business/2016/01/14/peel-police-violated-cellphone-customers-charter-rights-judge-rules.html.

and the CRTC's CCI rules that would enable government or law enforcement authorities to obtain CCI with a "simple request" from TSPs, as suggested by PIAC's Application.

22. PIAC's narrative about TSPs' lawful access practices, on which this entire proceeding rests, reflects a fundamental misconception about when and how TSPs' respond to lawful access requests. PIAC is raising and trying to address a problem that simply does not exist.

C. NO NEW REGULATORY MEASURES REQUIRED

23. Having failed to establish a sufficient nexus between TSPs and the COVID-19 Apps, in Part 8.0 of the Application, PIAC proposes (i) a new public health app related exception to the requirement to obtain express customer consent; and (ii) a corresponding process or regulatory test (the CADR) whereby TSPs must seek CRTC permission to disclose CCI to governmental authorities.[20]

24. CWTA opposes PIAC's proposals as they would not only create an unnecessary additional layer of privacy regulation, but also disrupt a mature and proven process.

25. For one, the proposals are completely unnecessary. PIAC has not provided any information to justify the proposals beyond unfounded speculation that government or law enforcement authorities are requesting subscriber information from TSPs in connection with the COVID-19 Apps.

26. Second, as described in detail above, even if TSPs were to receive such requests, TSPs already have comprehensive lawful access policies and procedures in place to receive, assess and respond to requests for CCI and personal information by government and law enforcement authorities in accordance with privacy laws and the CRTC's CCI rules.

27. Third, under PIAC's CADR process, it proposes that TSPs seek CRTC approval[21] for disclosures to governmental authorities on the basis of a "reasonable belief" that the subscriber information is necessary and essential in the circumstances to prevent, reduce or mitigate the spread of the serious illness of COVID-19.[22] With respect, the Commission does not have the requisite expertise to assess such public health-related requests.

28. Finally, we note that a Commission process to assess and approve any such requests would place the Commission and TSPs in conflict with legal processes that compel the production of information. For example, TSPs that fail to comply with a court order made pursuant to the *Criminal Code* without lawful excuse may be guilty of an offence.[23] It is also unclear how the

[20] PIAC Application, paragraphs 132, 147 and 151.
[21] PIAC Application, paragraph 147.
[22] PIAC Application, paragraph 147(a).
[23] See *Criminal Code,* s. 487.0199.

proposed process would work in practice for time sensitive requests or where the request is subject to a sealing order.[24]

29. PIAC's CADR process is a misguided solution in search of a problem and should not be approved or given further consideration. CWTA further notes that PIAC's solution appears to proceed on the basis that the current CCI rules apply only to wireline TSPs, that the definition of CCI is inadequately narrow and that TSPs disclose subscriber information pursuant to "simple requests". None of these assumptions are accurate. Among other things, CWTA notes that the definition of CCI is currently very broad and includes all information held by a TSP regarding the customer, other than the customer's name, address and a listed telephone number. This would include, for example, a subscriber's IP address information and transmission data.

30. In addition, contrary to PIAC's submissions, all TSPs, except providers of wireless services that are not switched, such as paging providers, must comply with the CRTC's CCI rules. This includes resellers of telecommunications services.[25]

31. As a result, CWTA submits that no new measures are required in respect of TSPs' collection, use and disclosure of Confidential Information, including any new Commission rules or processes regarding TSPs' handling of government requests for CCI.

D. CONCLUSION

TSPs play no role in the operation of the COVID-19 Apps. PIAC's Application does not raise any new facts to conclude otherwise. To the extent that the federal and provincial governments' collection and use of personal information in connection with the COVID-19 Apps is at issue in an appropriate case based on actual facts, PIAC has not demonstrated that current privacy frameworks are insufficient nor has it raised any credible concerns, issues or wrongdoing regarding the privacy practices of TSPs or the role of TSPs with regard to customer's privacy. As such, PIAC's Application should be dismissed with no further process.

*** End of Document ***

[24] See *Criminal Code,* s. 487.3(1).
[25] Telecom Regulatory Policy 2017-11, *Application of regulatory obligations directly to non-carriers offering and providing telecommunications services,* 17 January 2017.