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

4 May 2020

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

VIA GC KEY

Dear Mr. Doucet,

Re: *Application Regarding Pandemic Contact-Tracing at Application and Network Levels*

The Public Interest Advocacy Centre (PIAC) hereby files a Part 1 application requesting specific Commission action (as specified in the Application) in relation to all Canadian telecommunications service providers' involvement in potential or actual pandemic contact-tracing for public health purposes.

Please note that we bring this Application seeking clarity and transparency and not in any way seeking to impede appropriate public health measures.

Sincerely,

John Lawford,
Counsel to PIAC

cc All Canadian TSPs
Stephen Millington, CRTC

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; the Canadian Cable Systems Alliance; the Canadian Network Operators Consortium Inc.; Cogeco Communications Inc.; Comwave Networks Inc; Distributel Communications Limited; Freedom Mobile Inc.; Ice Wireless Inc.; Iristel Inc.; the Independent Telecommunications Providers Association (ITPA); Primus Management ULC; Quebecor Media Inc., on behalf of Videotron Ltd. (Videotron); Rogers Communications Canada Inc. (RCCI); Saskatchewan Telecommunications; Shaw Telecom G.P. (Shaw); TBayTel; TekSavvy Solutions Inc., Télébec, Limited Partnership; Telus Communications Company; etc., BEING ALL CANADIAN TELECOMMUNICATIONS SERVICE PROVIDERS

(RESPONDENTS)

REGARDING PANDEMIC CONTACT-TRACING AT APPLICATION AND NETWORK LEVELS

4 May 2020

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 pandemic contact-tracing at application and network levels by major Canadian telecommunications service providers (TSPs).

2. According to public news reports, the federal and certain provincial governments, on behalf of provincial and federal public health authorities, as well as municipal health authorities, are actively considering requesting that Canadian TSPs assist in tracking COVID-19 positive individuals in order to "contact-trace" them in efforts to control epidemic spread of the virus.

3. Such public news stories indicate a larger discussion of such telecommunications tracking facilities, likely largely through personal mobile wireless devices (smartphones) either by installing new software ("apps") whether with consumer/citizen consent or via operating software or other software upgrades to major smartphone operating systems and/or using network-level location tracing facilities of TSPs intended for wireless connectivity and network management.

4. This application asks the Commission to clarify that TSPs must follow the privacy requirements of the *Telecommunications Act*, to require all TSPs to notify the Commission of any steps taken for any government or private interest to facilitate contact tracing and to make those steps public, and to demonstrate the Commission's active oversight of this contentious area. PIAC believes the Commission's oversight role is crucial and that absent leadership and dedication to the rule of law, that there is a risk of corporate and governmental intrusion via Canadians' essential communications.

5. This application asks 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 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-

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

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.

6. The application is based on the principles of transparency, democracy and human rights and accountability. PIAC believes that the value of any such telecommunications-based contact-tracing system, coming at the very likely expense of confidentiality and consumer and citizen privacy, must occur in the fairest, most open and transparent manner, non-coercively and only for the intended purpose(s). Such applications and network systems must not inadvertently exacerbate social discrimination. PIAC also believes that any information or databases, algorithms or insights, should not be used for any extraneous commercial, government or other purpose as a result of any potential tracking, via apps or at the network level or both, and that any information or databases must be destroyed once such contact-tracing for this disease is no longer required.

2.0 THE PARTIES

7. 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.

8. The respondents are major retail mobile wireless service providers (WSPs) or Internet service providers (ISPs) or inclusively, "telecommunications service providers" ("TSPs").

9. While we have named certain of such providers above as examples in the interests of

administrative economy – the actual number of TSPs in Canada being very large – this application is however directed to all TSPs in Canada.

10. PIAC believes the Commission should provide guidance and rules to all TSPs, not just those named as respondents or to "major" TSPs. We have attempted to serve and otherwise bring to the notice of all TSPs of this application 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 the application to apply to them.

3.0 THE FACTS

11. It appears that the federal government[3] and several provincial governments and apparently at least one municipal government have been in talks or consultations with private companies to design smartphone-based contact-tracing in an effort to deal with the present COVID-19 epidemic.

12. Several contact tracing apps and network solutions have been approved or tolerated in other countries and require location tracking or, if not continuously transmitting location tracking, require the turning over of location from the app if the user has been deemed infected, quarantined or otherwise movement restricted or isolated.[4] These apps and network tracking systems vary widely in their technologies and presumably in their level of involvement with telecommunications service providers to work. Some operate at the device level and others have a measure of platform or operating system integration. Most prominent amongst these latter apps is the very recent Apple-Google COVID-19 "Privacy-Preserving Contact Tracing" program,[5] which: "In the second phase, available in the coming months, this capability will be introduced at the operating system

[3] Justin Trudeau, Press Conference, 25 March 2020: "We recognize in an emergency situation we need to take certain steps that wouldn't be taken in a non-emergency situation, but that is not something we are looking at now. But all options are on the table to do what is necessary to keep Canadians safe."

[4] Notably, Singapore – the "TraceTogether" app: "It uses Bluetooth Relative Signal Strength Indicator (RSSI) readings between devices across time to approximate the proximity and duration of an encounter between two users. This proximity and duration information is stored in an encrypted form on a person's phone for 21 days on a rolling basis. No location data is collected. If a person unfortunately falls ill with COVID-19, the Ministry of Health (MOH) would work with the individual to map out 14 days' worth of activity, for contact tracing. And if the person has the TraceTogether app installed, he/she is required by law (TraceTogether 2020) to assist in the activity mapping of his/her movements and interactions and may be asked to produce any document or record in his/her possession including data stored by any apps in the person's phone." Barry Sookman, "AI and contact-tracing: How to protect privacy while fighting the COVID-19 pandemic," Macdonald-Laurier Institute (April 2020). Australia appears to now promote a modified version of TraceTogether in that country.

[5] Apple Newsroom media release, "Apple and Google partner on COVID-19 contact tracing technology" (10 April 2020), online: https://www.apple.com/ca/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

level to help ensure broad adoption, which is vital to the success of contact tracing."[6]

13. However, it is possible that many such apps rely for their utility upon user location tracking, that may only be available to the app due to location tracking methods provided by the mobile wireless (*i.e.*, from WSPs) or (in the case of home WiFi use, or use in a WiFi zone out of the home) via the Internet (*i.e.*, from ISPs).

4.0 CONTACT-TRACING AND RELATED MATTERS

14. 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 social distance to slow the spread of the virus.

15. PIAC believes therefore that the present movement to develop COVID-19 contact-tracing primarily is responding to a public health inquiry into positive or suspected cases contact-tracing.

16. However, even such a "narrow" public health goal is related to and intertwined with related but purely public control measures, which can include: quarantine, self-isolation, social (or physical) distancing, essential services definitions, positive and negative testing prioritization and communications to governments and the public, and individual treatment, as well as potential anti-body testing and many related matters. The wide nature of potential consequences of public health contact-tracing and the legal and policy limits of public health as a discipline therefore complicates this purpose for any inquiry into individual privacy. We do not underestimate the complexity of such an undertaking nor the stakes of such an effort.

17. 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 and emergency management, 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 private employment, public order and policing perspective.

18. 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

[6] Apple, "Exposure Notification - Frequently Asked Questions" (April 2020), online: https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.0.pdf at p. 2.

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 the private sector raises serious issues that the Commission under its telecommunications oversight jurisdiction must consider not only in depth but in haste.

5.0 LAW: PRIVACY OVERSIGHT AND RULES FOR TSPS

19. We are concerned about the lack of action by the CRTC thus far on many matters during the present epidemic, but in particular its seeming failure, or at least failure of transparency if the Commission instead is working behind the scenes, to vet and manage the developing and very serious matter of the interplay of *Telecommunications Act* and other privacy-related requirements within its area of jurisdiction and the contact-tracing movement and its attempted integration into public health and emergency management. This lack of leadership and public accountability presents clear risks to consumer and citizen privacy and possibly makes the proposed contact-tracing solutions less reliable and more likely to be applied to unrelated uses.

20. Here is the law: the *Telecommunications Act* telecommunications policy objectives include subs. 7(i), which requires the Commission to consider how "to contribute to the protection of the privacy of persons.".

21. 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*.

22. 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.[7]

[7] 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.,

23. 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 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.

24. Therefore, we would expect that the Commission would inquire into the plans of TSPs regarding possible COVID-tracing apps and network usage (including location-tracking functionality). The Commission must remind the TSPs that, according to Commission interpretations of confidentiality of customer information and privacy that these TSPs would have to have obtained prior, verifiable, explicit consent from any customers to permit <u>any disclosure</u> of confidential customer information to any non-affiliated third party, as per the requirements of Telecom Decision 2003-33 and subsequent modifications made in Telecom Decision 2004-27, and Telecom Decision 2005-15.

25. This latter decision sets out the 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*

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

- *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.*

26. These new methods were added to the tariff rules on customer information confidentiality for telephony of the major incumbent telephone providers. For example, Bell Canada's General Tariff, No. 6716, which still applies to "regulated" telephone service areas in Bell Canada's "serving territory" of Ontario and Quebec reads thusly (Item 10: "Terms of Service", Article 11 "Confidentiality of Customer Records"[8]):

> 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 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

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

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.]

27. Before examining in detail the requirements of, and exceptions to, the Confidentiality Rules under these tariffs, PIAC acknowledges that these requirements apply to regulated telephony services of incumbent telephone 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.

28. 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, and not as a blanket permission that could apply to non-urgent, though still potentially life-saving matters such as pandemic contact-tracing.

29. 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 to facilitate public alerting for emergencies such as tornados and active shooters, but not generally for public health tracing. However, even if this exemption could be interpreted to include contact-tracing, it makes it clear that such a disclosure request must come from the (in this case) health authority and not some private actor such as a software vendor, and is limited to specific individuals being traced due to their relation with a confirmed or suspected positive COVID-19 patient and not as a general fishing expedition or blanket request to track all individuals in case one day they possible might be exposed to a positive case.

30. A final worry is the existence of previously consented 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.[9] In accordance with PIPEDA and, we submit, the telephone tariffs, such a "trove" or database of previous location and other data collected under prior consumer consent to location track mobile devices should not be provided to any private or government entities to build, improve or test COVID-19 tracing tools without the customer's new, explicit, prior individual consent for this new use or disclosure

31. Consumers and citizens have several legal, constitutional, ethical and democratically valid reasons for insisting that their TSPs protect their privacy to this degree: possible reduced civil liberties,[10] the creation of COVID-19 databases and their use in policing and emergency response,[11] and likely discriminatory use (against vulnerable or historically disadvantaged or oppressed groups and individuals) of tracking despite individual consent requirements.[12]

[9] See, for example, Appendix A for Rogers' Privacy Policy which allows such tracking with prior consent.
[10] See Canadian Civil Liberties Association, "CCLA Live COVID-Liberty Updates" and the links therein, online: https://ccla.org/coronavirus/
[11] 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
[12] 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",

32. 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" by law for pandemic control purposes in general.

33. 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 be permitted on a very strict, publicly transparent and time-limited basis and only for those purposes, with express consent. We would leave this determination, and the scope of and mechanics of any such permission, to the Commission.

6.0 CONCLUSION AND REQUESTED RELIEF

34. This application asks the Commission to, as a condition of offering telecommunications service (mobile wireless or Internet access) under ss. 7, 24, 24.1 and 47 and possibly s. 70, 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-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;

Policy Options, 30 April 2020. Online: https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/

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.

Yours truly,

John Lawford
Counsel for PIAC

jlawford@piac.ca
285 McLeod Street, Suite 200
Ottawa, ON K2P 1A1
(613) 562-4002
www.piac.ca
613-447-8125

7.0 ANNEX A: SAMPLE CUSTOMER-TRACKING CONSENT FOR MARKETING PURPOSES (ROGERS PRIVACY POLICY, EXCERPTS)

ROGERS PRIVACY POLICY
At Rogers, we are committed to protecting the privacy of the personal information of our customers and users of our digital properties. We take all reasonable steps to ensure that this information is safe and secure, including putting in place rigorous policies and procedures to fully comply with all Canadian privacy laws and regulations.
This Policy covers the following information:
• Scope and application;
• How we obtain your consent to collect, use and disclose your personal information;
• How and why we collect, use and disclose your personal information;
• Details on where your information is stored, secured and how long it is kept for;
• How to access your personal information that we hold; and
• Who to contact for queries about your privacy.
Scope & Application of this Policy
Who does this policy apply to? All customers and users of the products, services, websites, apps, and other digital services offered by Rogers and other members and affiliates of the Rogers Communications Inc. organization. These include our wireless services (Rogers, Fido, Chatr, Cityfone and its branded entities), Rogers Media brands, our Connected Home services (TV, Internet, Home Phone and Smart Home Monitoring), and Rogers for Business.
In some instances, our products and services or those offered by a third-party service provider to our customers or users have their own specific privacy policies.
[…]
What information does this Privacy Policy apply to? This policy applies to all personal information that we collect, use, or disclose about our customers and users of our digital platforms.
This includes your name, address, email, how you pay for your services, how you use our products including our websites, network use, and information gathered from third parties, such as credit bureaus. It also includes IP addresses, URLs, data transmission information, as well as the time you spend on websites, what advertisements you follow, and your time on and use of our apps.
[…]
Consent
How does Rogers obtain consent?
Your consent to the collection, use, or disclosure of personal information may be implied or express, through written, oral, electronic or any other method.
For example, when you provide us your address, it is implied that it is used for billing purposes and service provisioning. However, if we are dealing with more sensitive information, such a performing a credit check, we will seek your express consent. We will also obtain your express consent for marketing purposes.
[…]
How & Why We Collect Personal Information
How does Rogers collect my personal information?
[…]
Your information may be collected in the following ways:
• Automatically: When you use a product or service that we supply to you.
[…]
Why does Rogers collect my personal information?
Rogers collects personal information for many different reasons in order to provide you with the products and services we offer, including but not limited to the following:

- To deliver you the products and services you have purchased from us, and to bill you and collect payment for those products and services. To understand your needs and offer you products and services from members of the Rogers Communications Inc. organization including Rogers, Rogers Bank and our agents, dealers and related companies, or trusted third parties that may be of interest to you.
- To provide tailored service to you. For example, we may use account information about you to improve your interactions with us or provide a positive and personalized customer experience.
- To provide geo-location services that will send you offers and promotions from carefully chosen third parties based on your current and historical personal location information.
- To perform analytics, administer surveys, or request feedback to improve and manage our relationship with you.
- To ensure the Rogers networks are functioning and protect the integrity of our networks.
- To confirm or authenticate your identity and ensure your information is correct and up-to-date.
- To ensure compliance with our Terms of Service and Acceptable Use Policy.
- To comply with legal obligations and regulatory requirements.

[...]

[…]
Disclosure
When is my personal information disclosed?
Unless we have your express consent or pursuant to a legal power, we will only disclose your personal information to organizations outside Rogers without your consent in the following limited circumstances:

- To a person who, in our reasonable judgement, is seeking the information as your agent.
- To another telephone company, when the information is required for the provision of home phone service and disclosure is made confidentially.
- To a service provider or other agent retained by us, such as a credit reporting agency, for account management, the collection of past due bills on your account, or to evaluate your creditworthiness.
- To a service provider or third party that is performing administrative functions for us to manage our customer accounts.
- To another organization for fraud prevention, detection or investigation if seeking consent from you would compromise the investigation.
- To a law enforcement agency whenever we have reasonable grounds to believe that you have knowingly supplied us with false or misleading information or are otherwise involved in unlawful activities.
- To a public authority or agent of a public authority if it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of the information.
- To 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 the information.
- To a third party who may be interested in buying Rogers assets and personal customer information must be shared to assess the business transaction.
- We will disclose information about your credit behaviour to credit reporting agencies or parties collecting outstanding debt.
- Your personal information may also be shared with members or affiliates of the Rogers

Communications Inc. organization, such as Rogers Bank.

Storage, Security & Retention

Where will my personal information be stored?

Personal information about our customers or users of our digital properties may be stored or processed in or outside Canada. The information will be protected with appropriate safeguards, but may be subject to the laws of the jurisdiction where it is held.[13]

[….]

*** End of Document ***

[13] Underlined emphasis is PIAC's. Online: https://www.rogers.com/cms/pdf/en/Rogers-Terms-of-Service-Acceptable-Use-Policy-and-Privacy-Policy-en.pdf See for excerpts, at pp. 24-27.