TekSavvy Solutions Inc | 800 Richmond Street, Chatham ON N2M 5J5 | TELEPHONE 519.360.1575 | TOLL FREE 877.779.1575 | FAX 519.360.1716 | teksavvy.com

Bram Abramson
Legal & Regulatory

Direct Line 647.479.8093

babramson@teksavvy.ca

Professor Lisa Austin, Faculty of Law,
Professor Andrew Clement, Faculty of Information,
Professor Ron Deibert, Citizen Lab, and
Dr. Christopher Parsons, Citizen Lab,
University of Toronto;

Professor Colin Bennett, Department of Political Science
University of Victoria;

Professor Robert Diab, Faculty of Law
Robert Thompson University;

Professor Michael Geist, Faculty of Law and
Professor Valerie Steeves, Department of Criminology,
University of Ottawa;

Dr, Adam Molnar, Surveillance Studies Centre,
Queen's University;

Professor Andrea Slane, Faculty of Social Sciences & Humanities,
University of Ontario Institute of Technology; and

Professor Kevin Walby, Department of Criminal Justice,
University of Winnipeg.

VIA E-MAIL: <christopher@christopher-parsons.com>.

June 4, 2014

RE: January 20 Data Request (items 1-10); May 1 Personal Information Template

Dear Professors and Drs. Austin, Bennett, Clement, Deibert, Diab, Geist, Molnar, Parsons, Slane, Steeves, Walby, and Winseck:

As you know, TekSavvy Solutions Inc. ("TekSavvy") is a provider of Internet access, voice telephony, and related telecommunication services. On 20 January 2014, you forwarded an email setting out ten sets of questions and sub-questions about TekSavvy's information disclosure practices.

Part of the mission that TekSavvy has set for itself is to innovate in the protection of consumer rights online. Thus far, our focus has been on ensuring that we do so by providing an open, network-neutral, consumer-oriented service. However, the Edward Snowden leaks based in the U.S. and the multi-national investigative activity following them have helped underline a key commitment that is required to achieve this mission, which is strong data privacy and transparency. In part to better address challenges such as those raised by your letter, by Dr. Parsons' January 22 and March 6 Citizen Lab blog posts relating to it,[1] and a number of public disclosures that have come to light since then, TekSavvy has taken steps to strengthen our internal team dedicated to legal and regulatory matters.

In particular, we in April initiated a review of our privacy policy, consumer terms and conditions, and internal practices with respect to information that we treat as personal. This includes all of the information available to us that is about identifiable individuals, including unique device identifiers and metadata that are able to be correlated with an individual's or household's subscription. Our review involves a full audit of the systems that we have developed as our company has grown from a small access provider to its current size. The purpose of the review is to evaluate how our formal and informal collection, storage, and disclosure practices reflect our commitment and, where appropriate, to formalize our policies and practices in this regard, strengthen them, or both, including the issuance of regular transparency reports. The review is ongoing. Your questions and suggestions have been an important tool in focusing that review.

Because you asked that we respond by 3 March 2014, I would like first to apologise that we have not been able to do so until now. In view of overlap both in content and in audience, our answers are also responsive to a template published and publicized beginning May 1, when Citizen Lab advocated that Canadian telecommunications subscribers forward it to their providers in order to seek the personal information that their providers collect, retain, manage, and disclose about them. As you can imagine, a not-insignificant portion of our legal and regulatory resources have been devoted to process and responding to those template requests. General information about our policies and practices as they relate to that template is set out beginning on page 14 below, after the answers to your January 20 questions and sub-questions.

Q1. In 2012 and in 2013, how many total requests did your company receive from government agencies to provide information about your customers' usage of communications devices and services:

A1. In 2012, and 2013, we received 52 requests from government agencies about our customers' usage of communications devices and services. All of these requests were restricted to correlating Internet Protocol ("IP") addresses with subscriber name and information. All of them were received from law enforcement agencies.

Q1a) Within that total, please list the amount of requests your company received for each type of usage, including but not limited to: 1) Geolocation of device (please distinguish between real-time and historical); 2) Call detail records (as obtained by number recorders or by disclosure of stored data);

[1] Christopher Parsons, "Towards Transparency in Canadian Telecommunications", 22 January 2014, online: https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/, and "The Murky State of Canadian Telecommunications Surveillance", March 6, 2014, online: https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/.

3) Text message content; 4) Voicemail; 5) Cell tower logs; 6) Real-time interception of communications (i.e. wiretapping); 7) Subscriber information; 8) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.); 9) Data requests (e.g. web sites visited, IP address logs); 10) Any other kinds of data requests pertaining to the operation of your network and business.

A1a) All of those requests were received for 7) subscriber information. None of these requests were received for 1) geolocation, 2) call detail records, 3) text message content, 4) voicemail, 5) cell tower logs, 6) real-time interception, 8) transmission data, including duration of interaction, port numbers, and communications routing data, 9) data requests, including web sites visited, IP address logs, or 10) other kinds of data requests not covered by the categories you have indicated.

Q1b) For each of the request types, please detail all of the data fields that are disclosed as part of responding to a request.

A1b) For request type 7 (subscriber information), the data fields we disclosed were: subscriber name, postal address, telephone number, and e-mail address. All of these disclosures were made to government institutions acting with lawful authority in the context of a criminal investigation.

Q1c) Within the aforementioned total, how many of the requests were made for realtime disclosures, and how many were made retroactively for stored data?

A1c) Within the aforementioned total, all of the requests were made retroactively for stored data (subscriber name and contact details). None of them were made for real-time disclosures, nor related to information to which real-time disclosures would be relevant.

Q1d) Within the aforementioned total, how many of the requests were made in exigent circumstances, and how many were made in non-exigent circumstances?

A1d) The aforementioned total is for 2012 and 2013. During that period, we did not store information as to which requests were made in exigent, and which in non-exigent, circumstances. Rather, during that period it was our practice, consistent with sub-paragraph 7(3)(c.1)(ii) of *PIPEDA,*[2] to produce information where (a) pursuant to a lawful authority, (b) in the context of a law enforcement investigation, and (c) restricted to basic subscriber information.

Since that time, we have further restricted our practice as a result of the aforementioned review of all of our privacy policies and practices. It is now our policy to make such disclosures only in response to a warrant, production order,

---

2 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

or instances in which the conditions for such a warrant or order were present but exigent circumstances[3] prevented one from being obtained.

In relation to the above, we understand that draft legislation is currently before the Senate (Bill S-4) which, among other things, would revise subsection 7(3) of *PIPEDA.* These revisions would, irrespective of any findings the Supreme Court of Canada may make in the interim,[4] broaden the circumstances in which organizations may disclose personal information on their own initiative to third parties, and without a judicial order. The revisions would allow organizations to make such disclosures to government institutions or other organizations in relation to a contravention of laws that has been, is being, or about to be committed.[5]

It has been suggested that, had such legislation been introduced earlier, TekSavvy could have responded to the Voltage request[6] differently, such as by choosing to disclose the subscriber information that Voltage requested. To be clear, the policy described above was arrived at despite the draft legislation before the Senate. Should Bill S-4 be passed in its current format, it will not affect TekSavvy's approach to copyright matters.[7]

Q1e) Within the total, how many of the requests were made subject to a court order?

A1e) Within the total, one of the requests was made subject to a court order.

Q1f) Within the total, how many of the requests did your company fulfill and how many did it deny? If your company denied requests, for what reasons did it do so?

A1f) Within the total, we made 17 disclosures (33 percent) pursuant to lawful authority related to criminal investigations, and denied the remaining 35 (67 percent).

---

3 *Criminal Code,* R.S.C. 1985, c. C-4, section 487.11 ("A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, may, in the course of his or her duties, exercise any of the powers described in subsection 487(1) or 492.1(1) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant").

4 *Spencer v. the Queen,* Case 34644, Supreme Court of Canada, appealing *R. v. Spencer,* 2011 SKCA 144.

5 *Digital Privacy Act,* Bill S-4 (41st Parl., 2nd Sess), second reading (8 May 2014), subsections 6(8)-(10).

6 *Voltage Pictures LLC v. John Doe*, 2014 FC 161.

7 However, in the event Bill S-4 continues to move forward, TekSavvy intends to review whether Bill S-4's disclosure powers would affect our practice in the following scenario: we are approached directly by a non-Canadian police force in exigent circumstances, such as a U.S. police force acting on a live hostage or bomb threat traced back by an application provider to a TekSavvy IP address. As currently drafted, it is not clear that PIPEDA allows a telecommunications service provider to respond to such a situation without informing that individual in writing without delay of the disclosure, notwithstanding such disclosure's possible effect on the ongoing response to the live situation. Refer to *PIPEDA,* paragraph 7(3)(e), since a non-Canadian law enforcement agency is not a "government institution" as contemplated by sub-paragraph 7(3)(c.1)(ii): *Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers,* PIPEDA Case Summary 2008-394.

While we did not, for 2012 and 2013, store information as to the reasons for denial, please refer to A1d above with respect to our general practice. Non-exigent requests by a government institution that were not made *(i)* pursuant to a lawful authority, *(ii)* in the context of a law enforcement investigation, and *(iii)* restricted to basic subscriber information, would generally have been denied without a warrant or production order.

Q1g) Within the total, please identify how many requests were made by Federal, by provincial, and by municipal government agencies?

A1g) Within the total, 19 requests were by federal government agencies (37 percent). The remainder were made by provincial agencies, of which five were non-municipal (10 percent) and 28 were municipal (54 percent). These agencies were police forces.

Q1h) Do you notify your customers when government agencies request their personal information? If so, how many customers per year have you notified?

A1h) All government agency requests we have received for personal information have related to criminal investigations. Warrants and production orders generally prohibit notification of customers or disclosure of the warrant's or production order's existence to anyone. We have taken the position that the mere aggregation of warrants, production orders, and other requests received in order to enumerate them by relevant category would not in any way inform any third party of the content specific to, or specific existence of, any such judicial order.

We would note that in a non-criminal context, in response to a 2012 request by a third party for disclosure of subscriber information in a civil copyright matter,[8] we notified 2,114 subscribers that the subscriber name and contact details corresponding to their IP address had been requested by a rightsholder that had apparently tied those IP addresses to unauthorized peer-to-peer transfers of a particular film.

To date we have not released any subscriber information to that third party. The judicial order under which we are to do so, which followed lengthy court proceedings and ongoing follow-ups, limited the request to name and address information, and maintained strong court oversight as to how this information could be used and when it was required to be disclosed. We believe that this created an important protective framework for consumers.

Q2. For <u>each</u> type of usage in 1(a), how long does your company retain those records and the data fields associated with them?

A2. Q1a) asked about ten types of usage:

Q2.01) Geolocation of device (please distinguish between real-time and historical).

8 Please refer to note 6 above.

A2.01) We do not undertake geolocation of devices, such as through third-party IP address geolocation. We do undertake the following chain of activity:

(i) collect modem identifiers (Media Access Control ["MAC"] addresses) in order to authenticate their subscription;

(ii) associate IP addresses with those MAC addresses, in order to provide Internet access to them; and

(iii) insert those IP addresses into routing tables organized geographically, in order to route Internet traffic to and from those Internet access points.

Taken together, these data tables would permit geolocation of devices down to the community level. It is our policy, which we are now implementing, to maintain information that is in the correlation table outlined in (ii) for 30 days. This has been reduced from our previous retention policy, which is 90 days, as a result of the aforementioned review, and we are currently in the process of auditing our systems to ensure the universal deployment of this approach.

Q2.02) Call detail records (as obtained by number recorders or by disclosure of stored data).

A2.02) Call Detail Records ("CDRs") are call-level metadata records maintained in respect of voice telephony services. We currently provide two voice telephony services, both of them interconnected with the Public Switched Telephone System ("PSTN"): TekTalk, a managed voice-over-Internet service; and Home Phone, a dedicated primary exchange service. We do not have number record records for either service, but do have some stored data, as follows.

TekTalk generates CDRs only for long-distance calls, since local calls are not tolled, and our operational requirement for CDRs is billing-related. At present, those CDRs are archived indefinitely in order to support subsequent billing disputes and analysis and, more broadly, tax and anti-fraud requirements. Our policy review is currently engaged with determining the extent to which we can meet these requirements through aggregation that would allow the deletion of individual CDRs.

TekSavvy Home Phone is based on an Incumbent Local Exchange Carrier ("ILEC") wholesale service. Any CDR connected with a TekSavvy customer's use of TekSavvy Home Phone is generated and retained by the ILEC which, in turn, provides monthly billing records to TekSavvy. Like TekTalk toll CDRs, these billing records have thus far been archived indefinitely, which policy is subject to current review.

Q2.03) Text message content.

A2.03) We do not have text message records.

Q2.04) Voicemail.

A2.04) Deleted TekTalk voicemail messages can be retrieved by users for up to 14 days. We have not enabled functionality that would allow the onward storage or retrieval of voicemail messages deleted by the user. We do not store TekSavvy Home Phone voicemail messages, in respect of which we direct users to the third-party providers of these services.

Q2.05) Cell tower logs.

A2.05) We do not have cell tower logs.

Q2.06) Real-time interception of communications (i.e. wiretapping).

A2.06) We do not have real-time interception records.

Q2.07) Subscriber information.

A2.07) We retain subscriber information (subscriber name, street address, telephone number, email address where available, social media handles where available) and related billing information even after a subscription ends, in part in order to support the tax, anti-fraud, and related audit functions described earlier. We are currently reviewing our ability to shorten this period to two years after a subscription ends, based on the CASL[9] definition of an "existing business relationship", through techniques such as data de-identification and depersonalization.

We retain correlation tables linking subscriber information to device identifier, as described elsewhere in this response. It is now our policy to overwrite records in these correlation tables after 30 days.

Q2.08) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.).

A2.08) With respect to Internet access, we avoid logging transmission data that is personal information, such as IP-address-specific transmission data. The transmission data that we do retain in respect of IP addresses is the time and date on which the IP address began to be used (or "leased") and on which the lease expired due to prolonged inactivity. Apart from this information, and except where operational reasons require it such as for troubleshooting, we do not have further relevant transmission data outside the short window during which it is being read and written by our routing and switching equipment. Any such records retained for operational reasons are used only for that purpose and deleted as soon as is practicable.

Q2.09) Data requests (e.g. web sites visited, IP address logs).

---

9 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23, paragraph 10(10)(a).

A2.09) We avoid logging user data request records that are personal information, such as IP-address-specific web sites or other activity logs. Except where operational reasons require it, such as for troubleshooting, we therefore do not have relevant data request records outside the short window during which it is being read and written by our routing and switching equipment. Any such records retained for operational reasons are used only for that purpose and deleted as soon as is practicable.

Q2.10) Any other kinds of data requests pertaining to the operation of your network and business.

A2.10) The wholesale access services that are an input into our retail Internet access services are billed to us partly on the basis of capacity ("Capacity-Based Billing", or "CBB"). We therefore monitor our users' Internet data usage, which may be reflected on a given monthly bill depending on the package and options they have chosen for that month. This monitoring generates capacity usage records at regular intervals. The capacity usage records do not include port numbers, communications routing data, web sites visited, or other transmission data or metadata. They are aggregated for billing purposes, following which the individual records that have been aggregated are discarded as soon as is practicable.

Our Internet access service is bundled with domain name ("DNS") and email services. DNS requests are anonymized and are not logged. Our email services consist of Internet Message Access Protocol ("IMAP"), inbound Post Office Protocol ("POP3"), and outbound Simple Mail Transfer Protocol ("SMTP") services:

- Deleted IMAP and POP3 email messages that can no longer be retrieved by the accountholder are deleted, and no further metadata is stored in their regard—we have not enabled functionality that would allow the onward storage or retrieval of the email messages they have deleted.

- However, use of SMTP to send email generates metadata that is maintained for operational purposes, including spam filtering. At present, those SMTP logs are archived to support subsequent billing disputes and operations analysis, especially trouble-shooting. We are currently reviewing our ability to impose a rolling deletion window for these logs in respect of personal information without hampering operational purposes, such as through aggregation and de-personalization.

We maintain Web pages in order to provide information about our services and, in addition, are active on a range of social media platforms. We are currently reviewing our privacy practices in respect of these activities, particularly with regard to the log files that relate to IP addresses that visit our sites and with regard to our use of third-party marketing-related analysis tools like Google Analytics. Outside our use of third-party analysis tools, our correlation of IP addresses to subscribers is limited by the rolling 30-day window policy described above.

Q3. What is the average amount of time law enforcement requests for each of the information requests in 1(a) (e.g. 3-5 days of records)? What is the average amount of time that your company is typically provided to fulfill each of the information requests in 1(a)?

A3. Law enforcement requests that we receive typically relate to subscriber information, for which average time is not a relevant measure. We are typically provided 30 days to respond to a production order. We are asked to respond as soon as possible in exigent circumstances such as a hostage or bomb threat.

Q4. How many times were you asked to disclose information noted in 1(a) based specifically on:

Q4a) child exploitation grounds?
Q4b) terrorism grounds?
Q4c) national security grounds?
Q4d) foreign intelligence grounds?

A4. For 2012 and 2013, we did not store information as to which requests were made according to the classification set out above. It is our intent to do so going forward.

Q5. What protocol or policies does your company use to respond to requests for data that are noted in 1(a)?

To respond to requests for data that are noted in Q1a, we first determine whether the requester is a government institution or not. If they are not a government institution, we generally ask them to address themselves to one. If they are a government institution, we follow the legal standard set out in A5a.

Q5a) What legal standard do you require government agencies to meet for <u>each</u> type of data request noted in 1(a)?

A5a) Our general legal standard is to require that government agencies provide a warrant, provide a production order, or demonstrate that obtaining one is justified but unfeasible due to exigent circumstances, such as a live bomb threat.

You have asked how the legal standard that we require applies to each type of data request noted in Q1a, which asked about ten types of usage:

Q5a.01) Geolocation of device (please distinguish between real-time and historical).

A5a.01) We do not undertake geolocation of devices, such as through third-party IP address geolocation. We would apply the above-noted general legal standard in response to data requests for disclosure of the information set out in A2.01.

Q5a02) Call detail records (as obtained by number recorders or by disclosure of stored data).

A5a.02) We would apply the above-noted general legal standard to disclosure of stored CDRs that are in our possession. We do not have number recorder records.

Q5a.03) Text message content.

A5a.03) We do not have text message records.

Q5a.04) Voicemail.

A5a.04) We would apply the above-noted general legal standard to disclosure of stored voicemails that are in our possession.

Q5a.05) Cell tower logs.

A5a.05) We do not have cell tower logs.

Q5a.06) Real-time interception of communications (i.e. wiretapping).

A5a.06) We do not have real-time interception records.

Q5a.07) Subscriber information.

A5a.07) We would apply the above-noted general legal standard to subscriber information and IP-to-subscriber correlation disclosure.

Q5a.08) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.).

A5a.08) We do not generally have such transmission data. In the unlikely event that we do have it, as a result of trouble-shooting or other operational needs, we would apply our general legal standard to its disclosure.

Q5a.09) Data requests (e.g. web sites visited, IP address logs).

A5a.09) We do not generally have such data request records. In the unlikely event that we did have it, we would apply the above-noted general legal standard to its disclosure.

Q5a.10) Any other kinds of data requests pertaining to the operation of your network and business.

A5a.10) We would apply the above-noted general legal standard to data requests pertaining to the operation of our network and business.

Q5b) What are the average number of subscribers who typically have their information disclosed in government agencies requests, for each type of request noted in 1(a)?

A5b) The answers to Q1a noted that all of the requests we received in 2012 and 2013 from government agencies, to provide information about our customers' usage of communications devices and services, pertained to 7) subscriber information. None of these requests were received for 1) geolocation, 2) call detail records, 3) text message content, 4) voicemail, 5) cell tower logs, 6) real-time interception, 8) transmission data, including duration of interaction, port numbers, and communications routing data, 9) data requests, including web sites visited, IP address logs, or 10) other kinds of data requests not covered by the categories indicated.

Such requests from law enforcement agencies typically covered single subscribers. In response to your question as to the average number of subscribers who typically have their information disclosed in law enforcement agencies requests, the number therefore varies between zero and one. While Q1a and Q5b do not relate to government agencies requests for 2014, we have received one such request in 2014 that relates to more than one subscriber. It is the Federal Court order in respect of a copyright claim noted in A1d and A1h (Voltage), in respect of which no subscribers have had their information disclosed to date.

Q5c) Does your company have distinct policies to respond to exigent and non-exigent requests? If yes, what are these policies or how do they differ?

A5c) Yes. In non-exigent circumstances, it is our policy to require a warrant or production order. In exigent circumstances, it is our policy to (i) require that the government institution, generally a law enforcement agency, demonstrate that obtaining one is justified but unfeasible due to the circumstances; and to (ii) confirm the veracity of such demonstrations.

Q5d) Is your company required to design your networks and services so government agencies can more readily access customer data in a real time or in a retroactive manner? If yes, please detail those requirements.

A5d) TekSavvy does not provide mobile PSTN services subject to the *Solicitor-General's Enforcement Standards for Lawful Interception of Telecommunications.*

We are aware of *Criminal Code* provisions under which law enforcement requests could result in an order to provide for real-time interception or install tracking devices or number recorders,[10] *CSIS Act* provisions under which CSIS requests cold result in a real-time interception order,[11] *National Defence Act* provisions under which CSEC requests could result in a real-time foreign-communications interception order,[12] and *Child Pornography Reporting Act* provisions under which we could be required to preserve data at a secure offline

10 *Criminal Code,* sections 184.1, 194.2, 194.3, 185, 186 (telewarrant), 492.1 and 492.2.

11 *CSIS Act,* R.S.C, 1985, c. C-23, section 21.

12 *National Defence Act,* R.S.C. 1985, c. N-5, section 273.65.

location.[13] In the event we become subject to such orders, we may not have an avenue to be compensated for the costs of compliance unless "the financial consequences [are] so burdensome that it would be unreasonable in the circumstances to expect compliance."[14] We also anticipate the coming into force of, *Copyright Act* paragraph 41.26(1)(b) requiring us to retain records for six months—and, if a claimant commences proceedings during that period, one year after proceedings have been commenced—in respect of which regulatory provisions may provide a way to recover our compliance costs.

All of these provisions could create an incentive for TekSavvy to design its networks and services so that the cost of any mandatory orders can reasonably be absorbed. However, to date we have not acted on that incentive with respect to our network and services design.

Q5e) Does your company have a dedicated group for responding to data requests from government agents? Are members of this group required to have special clearances in order to process such requests? What is the highest level company official that has direct and detailed knowledge of the activities of this group?

A5e) Our company does not have a dedicated group for responding to data requests from government agents. We do not require employees to have special clearances in order to be available for processing such requests. Company officials at our company's highest levels have direct and detailed knowledge of our responses to data requests from government agents.

Q6. What is the maximum number of subscribers that the government requires you to be able to monitor for government agencies' purposes, for each of the information types identified in 1(a)? Have you ever received an official order (e.g. ministerial authorization court order, etc.) to expand one of those maximum numbers?

A6. Government agencies have not sought to require TekSavvy to undertake real-time monitoring of subscribers. Please see also A5b (above).

Q7. Has your company received inappropriate requests for information identified in 1(a)? If yes, why were such requests identified as inappropriate and who makes a decision that a request is inappropriate? And if yes, how did your company respond?

A7. TekSavvy denied 67 percent of requests received in 2012 and 2013 for the reasons set out in A1d and A1f (above). Although we did not, for 2012 and 2013, store information as to the reasons for denial, we did not generally receive requests from government institutions that had the appearance of being frivolous, for an improper purpose, or anything other than professional.

---

13 *Child Pornography Reporting Act,* S.C. 2011, c. 4, section 4.

14 *Tele-Mobile Co. v. Ontario,* [2008] 1 S.C.R. 305, paragraph 67.

Q8. Does your company have any knowledge of government agencies using their own:

Q8a) tracking products (e.g. 'IMSI Catchers')?
Q8b) infiltration software (e.g. zero day exploits, malware, such as FinFisher, etc.)?
Q8c) interception hardware (i.e. placed within or integrated with your company's network)?
Q8d) If yes to 8(a), (b), or (c), please explain.

A8. We do not have any experience of government agency tracking products, infiltration software, or interception hardware on our network.

Q9. Does your company cooperate with government agencies that use their own tracking equipment or provide information on how to interoperate with your company's network and associated information and subscriber information? If yes, how does it cooperate, how many requests does it receive for such cooperation, and how many of your subscribers have been affected by such equipment or interoperation?

A9. No, we do not cooperate or provide the kind of information referred to.

Q10. In 2012 and 2013, did your company receive money or other forms of compensation in exchange for providing information to government agencies? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?

A10. No, we did not receive compensation in 2012 and 2013 for providing information to government agencies.

Q10a) Does your company charge different amounts depending on whether the request is exigent or non-exigent? Does your company charge fees for exigent cell phone tracking requests from law enforcement authorities?

A10a) Please refer to A10.

Q10b) Please include any written schedule of fees that your company charges law enforcement for these services?

A10b) We are aware of ILEC Law Enforcement Agency Services ("LEA Service") tariffs establishing charges for Customer Name and Address and for Service Provider Identification Service requests relating to telephone numbers.[15] TekSavvy, whose services are not tariffed, has not created any similar schedule of fees. In any case, our current policy of requiring a warrant, production order, or exigent

[15] *Provision of subscribers' telecommunications service provider identification information to law enforcement agencies*, Order CRTC 2001-279, 30 March 2001; *Provision of subscribers' telecommunications service provider identification to law enforcement agencies,* Telecom Decision CRTC 2002-21, 12 April 2002.

circumstances, which is described in A1d and A5c above, limits the circumstances in which imposition of a fee schedule is likely possible.

Q10c) Does your company operate purely on a cost recovery basis for providing information to government agencies?

A10c) Please refer to A10. In the past the combined volume of private information requests, from government agencies seeking third-party information and from individuals requesting records containing their own information, has not required in-depth review of costs incurred. We are now reviewing these costs in the context of the aforementioned policy review.

The above-noted questions were posed, and our answers to them provided, in part in order to tell you about our data retention and sharing policies. On 1 May 2014 Citizen Lab published a blog posting entitled "Responding to the Crisis in Canadian Telecommunications". The blog posting argued that Canadians ought to fill in a provided template and issue it to the telecommunications companies providing them with service. The blog posting suggested that doing so would help Canadians improve their ability to understand how companies manage the personal information entrusted to them and then make informed decisions about whether they want to maintain that commercial relationship.[16]

As a telecommunications company providing Canadians with service, we have received many such template requests, whose content relates to the above-noted questions and answers. In view of the overlap between your 20 January 2014 letter and Citizen Lab's 1 May 2014 blog posting, we are therefore providing further information that is responsive to the Citizen Lab template, relating the information it seeks to the answers set out above. It is our intent that the review we have initiated of our privacy policy, consumer terms and conditions, and internal practices result in the making available of this information to our users in a readily-accessible format. It is our hope that, in the interim, including it in this published letter will be of assistance.

T1. All logs of IP addresses associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers).

T1(R). We log the IP addresses associated with the MAC addresses that correspond to particular devices, and log which of those devices are associated with particular customers, in the manner described in A2.01.

It is our policy to retain the IP-to-MAC-address correlation information for 30 days. As described in A2.08 and A2.09, we do not store information as to the IP addresses or domain names of sites that subscribers visit or their times, dates, or port numbers.

T2. Listing of 'subscriber information' that you store about me, my devices, and/or my account.

---

[16] Christopher Parsons, "Responding to the Crisis in Canadian Telecommunications", 22 January 2014, online: https://citizenlab.org/2014/05/responding-crisis-canadian-telecommunications/.

T2(R). Our subscribers can access much of the information that we store about them online through TekSavvy's My Account portal, including name, address, service address, phone number, email address, usage information, and past bills. The subscriber information that we store that cannot yet be accessed through the My Account portal consists generally of:

- modem type, firmware, and MAC address;
- current-billing-cycle usage information;
- communications opt-ins; and
- internal notes on file, including call logs.

Please also refer to the answers provided above, particularly A2.07, A2.10, and A5a.07.

T3. Any geolocational information that you may have collected about me, my devices, and/or associated with my account (e.g. GPS information, cell tower information).

T3(R). As we do not provide mobile services, we do not have GPS or cell tower information, nor undertake targeted geolocation of devices. However, please refer to A2.01 above with respect to routing table information that could geolocate a subscriber's device down to the neighbourhood.

T4. Text messages or multi-media messages (sent and received, including date, time, and recipient information).

T4(R). As we do not provide mobile services, we do not have text ("SMS") or multimedia ("MMS") messages. We do provide voicemail and email services, which are addressed above at A2.02 and A5a.04 (voicemail) and A2.10 (email), respectively

T5. Call logs (e.g. numbers dialed, times and dates of calls, call durations, routing information, and any geolocation or cellular tower information associated with the calls).

T5(R). We maintain logs for operational purposes whose information is deleted after one week. We also maintain last-ten call information (last ten calls missed, answered, and dialed, respectively) that is available, if applicable, in the My Account portal. However, most call logs and the related data fields described in parentheses are stored either in Call Detail Records that we retain, and in billing records. Our treatment of CDRs is set out above in A2.02. Our treatment of bills is set out above in T2(R).

T6. Information collected about me, or persons/devices associated with my account, using one of your company's mobile device applications.

T6(R). Our company does not have mobile device applications.

T7. Any additional kinds of information that you have collected, retained, or derived from the telecommunications services or devices that I, or someone associated with my account, have transmitted or received using your company's services.

T7(R). All of the kinds of information that we routinely collect, retain, or derive are described in the answers included in this letter. Please refer, in particular, to A2.01 through A2.10, which address related issues.

T8. Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies.

T8(R). Our approach to such disclosures is addressed above at A1h.

We trust that the information we have provided in this letter responds to your questions. As noted, this information is part of an ongoing process at TekSavvy. We work to ensure that all of our practices comply with our *PIPEDA*[17] and CRTC[18] obligations. However, we have come to believe that it is also TekSavvy's responsibility, as part of its understanding with its subscribers and as part of the value it delivers to Canadian telecommunications markets, to lead with respect to going beyond those obligations.

While that process is ongoing, we are glad to have embarked upon it, and would be pleased to continue this dialogue with you as we further refine our policies and practices in this area.

Yours sincerely,

[transmitted electronically]

Bram Abramson
Chief Legal and Regulatory Officer

---

17 Cited above, at note 2.

18 We note, in particular, the confidentiality provisions requiring that, unless a customer provides express consent or disclosure pursuant to a legal power, information other than the customer's name, address, and listed telephone number is not to be disclosed to anyone but: *(a)* the customer or *(b)* their agent; another *(c)* telephone company or *(d)* service provider, for operational purposes and provided it is on a confidential basis; or *(e)* a collections agent, again on a limited basis. *Confidentiality provisions of Canadian carriers,* Telecom Decision CRTC 2003-33, 30 May 2003, paragraph 49, as extended by *Follow-up to Telecom Decision CRTC 2003-33 – Confidentiality provisions of Canadian carriers,* Telecom Decision CRTC 2004-27, 22 April 2004, paragraph 22.