TekSavvy Solutions Inc. 800 Richmond Street, Chatham, ON N2M 5J5 | 227 rue Montcalm, Gatineau, QC J8X 2G9 | www teksavvy.com | tel 1-877-779-1575

Andy Kaplan-Myrth
VP, Regulatory and Carrier Affairs
akaplanmyrth@teksavvy.ca tel +1 819-484-1205

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

10 November 2017

RE: Updated data request

Dear Dr. Parsons:

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, to which we responded on 4 June 2014. We understand that that response became the first transparency report issued by a Canadian telecom service provider.

In our response we indicated that part of the mission TekSavvy had set for itself was to innovate in the protection of consumer rights online. Our focus, we noted, had been on ensuring we do so by providing an open, network-neutral and consumer-oriented service. But the equally important role of strong data privacy and transparency had become increasingly clear, and we noted changes that TekSavvy had taken to strengthen its internal team dedicated to legal and regulatory matters, including a review of our privacy policy, consumer terms and conditions, and internal practices with respect to information we treat as personal.

Thank you for your letter, dated May 12, 2017, updating your questions of 2014 and requesting that we update our response. We are pleased to do so. Three years later, neither net neutrality nor data privacy can be said to have receded from public consciousness. In that regard we note, among many other recent events, the Consultation on National Security convened by the Ministers of Public Safety and Emergency Preparedness, and Justice between September and December 2016. Our response in that Consultation addresses a number of the issues raised in your update request.[1]

Q1. In 2014, 2015 and 2016, how many total requests did your company receive from government agencies to provide information about your customers' usage of communications devices and services?

Q1c) Within the total number of requests described in question 1, how many (ii) were made in exigent circumstances, and how many were made in non-exigent circumstances; (iii) were made subject to a court order, and (v) were made by federal, by provincial, and by municipal government agencies?

---

1 TekSavvy response to Ministers Goodale and Wilson-Raybould , *RE: Consultation on National Security*, 15 December 2016, <https://www.documentcloud.org/documents/3243036-Consultation-on-National-Security-TekSavvy-2016.html>

A1. In 2012-2013, TekSavvy logged 52 requests from government agencies about our customers' usage of communications devices and services, all from law enforcement agencies seeking to correlate Internet Protocol ("IP") addresses with subscriber name and information. In 2014, 2015, and 2016, TekSavvy received at least 235 similar requests from government agencies.

This includes court orders, demands in emergency circumstances, and formalized "jurisdiction requests", which are documents created according to internal law enforcement procedures. It does not include most informal contacts requesting information: those are difficult to log since they tend to be brief emails and, rather than a formal response, are usually responded to simply by explaining our procedures.

In the same way, this figure does not include preservation demands made by a peace officer under section 487.012 of the *Criminal Code,* nor preservation orders of a court extending the duration of those demands. Preservation demands and orders were formalized and given specific and limited durations in the 2014 changes to the *Criminal Code.* They are an important tool by which law enforcement can, and does, ensure that evidence can be preserved without delay in a way that allows a justice of the peace to test the need to disclose personal information, as against privacy rights, without impeding an investigation.

The following is a breakdown of the above-noted data, with additional details responsive to some of the related questions that were combined with this one (1(c)(ii)-(iv)):

	2014	2015	2016
Production orders (Criminal and national security)	**20**	**48**	**50**
Federal	3	6	20
Provincial	0	5	1
Local	17	37	29
Exigent circumstances	**4**	**14**	**11**
Civil matters (Norwich Orders)	**1**	**1**	**0**
Jurisdiction requests	**29**	**37**	**20**

Of these requests, 29 (4, 14, 11) were thus made in emergency circumstances, and 119 were subject to a court order (including 118 production orders, and excluding one civil summons that was not a court order).

Breaking down the requests by jurisdiction, 30 (4, 6, 20) were federal, including one Norwich Order;[2] six (0, 5, 1) were provincial; and 83 (17, 37, 29) were local. Court orders that were federal or resulted from federal law enforcement therefore accounted for 25 percent, provincial for 5 percent, and local for the remaining 70 percent.

Q1a) Within that total number of requests, please list the amount of requests that 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

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

disclosure of stored data); 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 (i.e. duration of interaction, port numbers, communications routing data, etc.); 9) data requests (i.e. websites visited, IP address logs, jurisdiction requests); and 10) any other kinds of data requests pertaining to the operation of your network and business.

Q1b) For each of the request types listed in question 1(a), please detail all of the data fields that are disclosed as part of responding to a request.

A1ab) Requests that we receive sometimes seek information from more than one category listed in Q1a). However, every request sought basic subscriber information (type 7), including the address to which the subscriber's service was provisioned (type 1).

For these requests, the information disclosed depends on the information requested.,

There is no standard for what law enforcement agencies request in production orders. Managing requests that ask for different types of information, referring to different data points by different names, is a continuing challenge for us. One law enforcement agency that sends a significant number of requests has standardized the following language, which we have found allows us to process their requests more efficiently:

> "subscriber information, specifically the subscriber name, physical address, and phone number associated to the IP address ###.###.###.### on January 1, 2017 at 13:50:00 UTC."

We understand the term "subscriber information" to mean subscriber name, telephone number, and service address, and disclose only this information in response; and, with respect to service address, provide the street number, street name, city, province, and postal code as well as any apartment or unit number where relevant.

Because TekSavvy does not provide mobile wireless services, information type 5 (cell tower logs) did not pertain to us. Of the remaining information types (2, 3, 4, 6, 8, 9, 10):

- *Types 2 (call detail records), 3 (text message content), 4 (voicemail):* None of the above-noted requests related to call detail records or voicemail.

- *Type 6 (wiretapping):* None of the above-noted requests related to real-time wiretapping. However, one request related to the following unusual circumstance, which originated internally. In 2016, a domestic violence incident was overheard by our agent while on the phone with a customer, and was referred to law enforcement. As TekSavvy indicates in the greeting message that customers hear when they call in, we record our calls to create a record of what we've agreed to verbally with callers. The

subsequent investigation requested the call recording from TekSavvy; the investigating officer was invited to obtain, and did obtain, a production order in respect of that recording; and TekSavvy disclosed the recording to the investigating officer.

- *Type 8 (transmission data):* Transmission data includes data that relates to routing or signalling that is transmitted to identify, activate or configure a device to establish its access to a telecommunications service, but does not reveal the substance, meaning, or purpose of the communication. We therefore take transmission data to include the MAC addresses of cable modems, and the logins of DSL modems, that are used to establish a three-way connection between an end-user, a wholesale network access provider's IP (cable) or Point-to-Point over Ethernet (PPPoE) (DSL) transmission path, and TekSavvy.

  Many of the above-noted requests included this type of transmission data as part of a broader request relating to equipment used. When required, we provided that information. If required, we may also provide the make, model, and serial number of equipment, which TekSavvy retains in respect of modems in order to provision services and better troubleshoot modem incompatibility, a frequent technical support issue. Since it is needed to provision and troubleshoot services, we retain this information both for equipment we have sold and for cable modems supplied by the customer.

- *Type 9 (data requests, including IP address logs and jurisdiction requests):* As indicated on the table above, we received 86 jurisdiction requests in 2014-2016 (29, 37, 20).

  We received 26 (4, 14, 8) requests that sought to identify all IP addresses previously held by the subscriber who was correlated to the IP address and time stamp provided in those production orders. The additional data fields disclosed as part of responding to a compelled request of this nature are, for dynamic IP addresses, the observed start and end time and date of the session during which the dynamic Internet Protocol address was leased during TekSavvy's retention window.

- *Type 10 (other data requests pertaining to our network or business):* We take this to include requests seeking payment records, account information, and correspondence. We received 44 (7, 20, 17) requests of this type.

Certain kinds of requests were frequently the precursor to a subsequent request—in particular, jurisdiction requests (type 9), which typically pertained to an item for which a production order was to be sought.

Q1c) i. Within the total number of requests described in question 1, for real-time disclosures, and how many were made retroactively for stored data?

A1c) i. None related to real-time disclosures, nor related to information to which real-time disclosures would be relevant.

Q1c) iv. Within the total number of requests described in question 1, how many of the requests did TekSavvy fulfill and how many did it deny? If TekSavvy denied requests, for what reasons did it do so?

A1c) iv. Within the total (235), we made 109 compelled disclosures. We note that the total number of requests described in question 1 pertains to the number of formal requests we received and logged but, as explained more fully in the response to question 1, less-formal requests were not generally logged. We took time to explain lawful authority procedures to less-experienced law enforcement representative on a number of occasions including, in some instances, directing them to more-experienced colleagues.

Production orders properly issued by a court were in most cases fulfilled even where, as on a number of occasions, their fulfillment consisted of an affidavit confirming the absence of responsive records. In certain circumstances, we did have occasion to suggest to law enforcement that as the order they had sought and obtained might be overbroad in a way that could invite a challenge, they might be well-served to seek its revision, and they were successful in having them rescinded and replaced: these activities, which were difficult to track, are not reflected in the numbers above. We frequently have to seek clarification as to the issuing Justice of the Peace, whose signature is not legible. Finally, on four occasions, production orders served on TekSavvy were irregular or non-compliant in a way that caused them not to be compelled pursuant to lawful authority.

Where exigent circumstances are raised by someone other than a peace officer as defined in the *Criminal Code,* we must deny their request, and direct them to a peace officer. Exigent circumstances requests raised by law enforcement are required to include the following information, which is evaluated to ensure that the information sought is required to prevent bodily harm or death to a person, that the circumstances in which a production order would ordinarily be provided are present, but that it is impracticable to obtain a court order:

a) IP address inquired about;

b) date and time, as precisely as possible, at which the IP address was associated with the emergency;

c) personal information requested (for example, name and service address associated with the IP address at that date and time);

d) name of the law enforcement agency making the request.

e) occurrence number giving rise to the request;

f) brief explanation of why it is impracticable to obtain a court order;

g) how the information requested will assist in avoiding the imminent bodily harm of concern;

h) name, rank, badge number, and contact information of the requesting officer;

i) name, rank, and contact information for the officer in charge of the investigation; and

j) name, rank, and contact information for the commander of that officer's unit or division with a rank of at least Sergeant, and statement as to whether that commander is aware of the request being made.

Jurisdiction requests are not fulfilled as they are not compelled pursuant to lawful authority. Our response to the recent federal Consultation on National Security, cited above, suggests procedures that we believe would be more effective and avoid reliance on instruments of this type. At the same time, we generally point those making jurisdiction requests to the specific processes for the preservation and production of data provided for by the *Criminal Code.*

Q1d) Did you notify your customers when government agencies requested their personal information? If so:

Q1d)i. when did you notify them (i.e. at the time of or after the requests were made?)

A1d)i. We notified our customers who had their information disclosed to government agencies as soon as feasible, unless compelled not to. We are compelled not to make such disclosures under two kinds of circumstance.

First, we may have been served with a non-disclosure order prohibiting the disclosure of the contents or existence of the production order to which they relate for a set period of time. When a non-disclosure order is present, we do not inform the affected end-user until the non-disclosure order has expired. Where its expiry is not imminent or is indefinite, we check in with the law enforcement officials who obtained the non-disclosure order to verify whether it can be rescinded.

Second, we must ensure that the disclosure would not interfere with an on-going investigation. This is, again, the subject of ongoing communication with law enforcement.

Q1d)ii. how many customers per year have you notified?

A1dii) In 2014 we notified two customers; in 2015, 13 customers; and in 2016, 21 customers. There are still a number of time-limited non-disclosure orders pertaining to requests made in 2016, and indeterminate non-disclosure orders pertaining to requests for a broader period, generally until investigation is complete and the matter settled. In those cases, which are frequent, we are prevented from informing affected end-users at all, but continue to follow up with the appropriate law enforcement agency.

Q2. For each type of usage listed in question 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).

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), for cable modems, and DSL logins, for DSL modems, in order to authenticate their subscription;

(ii) associate (DSL) or record the association of (cable) IP addresses with those identifiers, 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, while the street addresses of the services to which the devices connect are already in our systems.

We require the information that is in the correlation table outlined in (ii) for 30 days after the IP address lease has ended. We may therefore have information about an IP address lease from more than 30 days if the session continued to be open for a period exceeding 30 days.

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

A2.02) 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 Protocol (VoIP) service; and Home Phone, a dedicated primary exchange service.

TekTalk generates CDRs for all calls, both local and long distance. At present, those CDRs are archived indefinitely in order to support subsequent billing disputes and analysis and, more broadly, tax and anti-fraud requirements.

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 by the ILEC which, in turn, provides monthly billing records to TekSavvy. The ILEC collects and stores five months of long-distance CDRs and does not collect or store any CDRs in relation to local calls. Once the long-distance CDRs are provided to TekSavvy for billing purposes, they are stored indefinitely.

Aside from the services we offer, TekSavvy uses voice telephony services to communicate with our customers. All calls to TekSavvy are recorded and the subsequent CDRs are stored for a period of two years to assist in the resolution of service-related or billing disputes.

Q2.03) Text message content.

A2.03) We do not offer text messaging services. However, we have recently started to use text messaging to communicate with our customers. Currently, this text message content is stored indefinitely.

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 retain correlation tables linking subscriber information to device identifier, as described in A2.01. Records in these correlation tables are deleted 30 days after the IP address lease expires.

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

A2.08) Please see A2.01 concerning the retention of information related to cable and DSL sessions. Non-session-related MAC address, DSL login, and account-specific volume-related transmission data summaries are retained indefinitely. Invoices, which include summaries of volume of data transfer, are also retained indefinitely.

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

A2.09) The functionality which enables the collection of information about Web sites visited is not currently enabled, however, test information for a sample of users was in the past, maintained and quarantined within a small network engineering team as a byproduct of their work with the equipment that meters traffic usage. This information has since been purged. There is no intent to enable this functionality going forward.

With respect to IP address correlation information, please refer to A2.01, subject to the requirement to preserve for six months correlation information in respect of which a notice of claimed infringement with all required identifiers has been received under the *Copyright Act.* We fulfill this obligation.

We currently retain jurisdiction requests for an indefinite period, but do not compile personal information related to them.

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

A2.10) We 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 are aggregated for billing purposes, following which these summarized records are stored indefinitely.

As noted above, we previously collected, maintained and quarantined information for a sample of users within a small network engineering team as a byproduct of their work with the equipment that meters traffic usage. This information was not used and has been purged.

Our Internet access service is bundled with domain name ("DNS") and email services. DNS requests are anonymous 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 maintain Web pages in order to provide information about our services and, in addition, are active on a range of social media platforms. 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.

Phone call recordings are purged after two years, but our written correspondence with our customers, including ticket notes and other account information, is currently retained indefinitely. So are payment records, which include amount paid, account number, internal invoice number, and internal batch number, which support payment dispute and anti-fraud resolution. However, credit card information is purged 24 hours after the account has been cancelled.

Q3. What is the average amount of time law enforcement requests for each of the information requests referred to in question 1(a)? What is the average amount of time that your company is typically provided to fulfill each of the information requests in question 1(a)?

A3. Law enforcement requests that we receive typically relate to subscriber information, for which intervals are not a relevant measure. We are typically provided 30 days to respond to a production order, and we respond within that time. We are asked to respond as soon as possible in exigent circumstances such as missing children; we do not have sufficient volume of these requests to calculate a meaningful average, but generally respond within 30 minutes.

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

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

A4. While we did not categorize requests according to the classification set out above in 2014, 2015, and 2016, we were most often asked to disclose information referred to in Q1a in situations *(a)* alleged to involve child exploitation. We received *(b)* at least one request in each of 2014 and 2015 relating to terrorism; *(c)* at least two requests in 2014, and one in 2015, relating to national security; and *(d)* at least six requests in 2014, one in 2015, and three in 2016, relating to fraud.

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

A5. To respond to requests for data that are noted in Q1a, we first determine whether the requester is a domestic government institution or not. If they are not a domestic government institution, we generally ask them to address themselves to one. If they are a domestic government institution, we follow the legal standard set out in A5a.

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

A5a) Our general legal standard is to require that government agencies demonstrate that the disclosure is compelled pursuant to lawful authority, in the manner clarified by *R. v. Spencer*,[3] either by producing a warrant or production order, or demonstrating that obtaining one is justified but unfeasible due to exigent circumstances, such as a missing child.

You asked how the legal standard that we require applies to each type of data request noted in Q1a. We apply that legal standard to every such type.

---

[3] *R. v. Spencer,* [2014] 2 SCR 212, paragraphs 63-66 and 71-74.

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

A5b) The answers to Q1a noted that the majority of the requests we received in 2014, 2015, and 2016 from government agencies, to provide information about our customers' usage of communications devices and services, pertained to subscriber information (request type 7).

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.

The single request in 2014 that was not from a law enforcement agency sought to have Teksavvy disclose subscriber information for more than two thousand customers. We have not disclosed any such information to date in relation to this request.

Q5c) Does TekSavvy 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 that such demonstrations are true. The means by which we do so is set out in A1c)iv.

Q5d) Is TekSavvy 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 is required, pursuant to paragraph 41.26(1)(b) of the *Copyright Act,* to retain correlation records for six months and, if a claimant commences proceedings during that period, one year after proceedings have been commenced, in respect of accounts in respect of which a notice of claimed infringement has been received.

A recent *Federal Court of Appeal* decision established the manner and form in which this customer data may be accessed as follows: it must be

> in a manner and form that can be used by the copyright owner to determine its options and, ultimately, by the court to determine issues of copyright infringement and remedy….
>
> An indecipherable jumble of randomly arranged records that copyright owners and courts cannot figure out will not, in the words of paragraph 41.26(1)(b), "allow [copyright holders and courts to determine] the identity of the person to whom the electronic location belongs." The records must

also be retained in a manner that can be disclosed promptly. Only the prompt provision of helpful, usable records to copyright owners and ultimately to the courts fulfils the purposes of the legislative regime and the broader purposes of the *Copyright Act.*[4]

TekSavvy does not use licensed spectrum or 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 installation of tracking devices or number recorders,[5] CSIS Act provisions under which CSIS requests could result in a real-time interception order,[6] National Defence Act provisions under which CSEC requests could result in a real-time foreign- communications interception order,[7] and Child Pornography Reporting Act provisions under which we could be required to preserve data at a secure offline location[8], and Copyright Act provisions requiring us to retain records identifying a subscriber upon receiving a notice of claimed infringement[9]. 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."[10]

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 or legal training 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) TekSavvy's Legal, Regulatory and Public Policy (LRPP) department houses TekSavvy's Data Protection Office, which is the group dedicated to responding to data requests from government agencies. Each member of this group has training in our privacy policies and in handling data requests. TekSavvy's VP, Regulatory and Carrier Affairs is a member of the Data Protection Office and has

---

4 *Voltage Pictures, LLC v. John Doe*, 2017 FCA 97, paragraphs 38-39.

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

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

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

8 *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, S.C. 2011, c. 4, section 4.

9 *Copyright Act*, R.S.C., 1985, c. C-42, section 41.26(1)(b).

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

direct and detailed knowledge of the activities of the group, including 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 question 1(a)? Have you ever received an official order (i.e. ministerial authorization court order, etc.) to expand one of those maximum numbers?

A6. Government agencies have not sought to require TekSavvy to undertake subscriber monitoring.

Q7. Has your company ever received inappropriate requests for information identified in question 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. 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. However, in our view, in ordinary circumstances, only compelled disclosure adjudicated by a body such as a court is appropriate, and it is inappropriate to expect that a neutral intermediary such as an ISP ought to be the locus of such decisions. In that sense, any request that is not accompanied by lawful authority demonstrating that it is a compelled disclosure is inappropriate.

Some production orders that we have received have included a condition that prohibits us from disclosing or permitting disclosure of the content, existence or operation of the order. Since a judge or justice can now issue a non-disclosure order that accomplishes the same goal, in our view it is inappropriate for the order itself to include a condition prohibiting disclosure. When we receive production orders that include such conditions, we ask the requesting officer to revise the order and seek a non-disclosure order instead. We could apply to the court to revoke those conditions, and we may do so in the future; to date, we have not made such an application.

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

Q4a) tracking products (i.e. IMSI Catchers)?

Q4b) infiltration software (i.e. zero day exploits, malware, such as FinFisher, etc.)?

Q4c) interception hardware (i.e. placed within or integrated with your company's network)?

Q4d) If yes to question 8(a), (b), or (c), please explain.

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, and how many requests does it receive for such

cooperation, and how many of your subscribers have been affected by such equipment or interoperation?

A8-9. No, we do not have specific knowledge of these beyond what is reported in the press.

Q10. In 2014, 2015 and 2016, 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 listed in question 1(a)?

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?

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

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

A10-10c. We do not receive compensation for providing compelled information. 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.[11] TekSavvy, most of whose services are not tariffed, has not created any similar schedule of fees: nor is it clear what leverage TekSavvy could have to demand a fee for information whose provision is compelled by law.

Yours sincerely,

[transmitted electronically]

Andy Kaplan-Myrth
VP, Regulatory and Carrier Affairs

cc: Stephanie Miller—Privacy and Transparency Associate

---

11 *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.