TekSavvy Solutions Inc.

First Quarterly Transparency Report

Reporting period: January 1, 2017 to March 31, 2017

Published October, 2017

Introduction

Welcome to TekSavvy's first quarterly transparency report! The purpose of this report is to provide insight into our disclosure practices by detailing how often we receive or respond to government agencies' requests for the personal information of our end users.

This particular edition of our Transparency Report discloses information about requests that we received between January 1, 2017 and March 31, 2017. As of the date when this report was published, at least six months have passed since we responded to each of those requests.

The Government of Canada has endorsed the development and issuance of transparency reports. Innovation, Science and Economic Development Canada's (ISED) have subsequently developed Transparency Reporting Guidelines. Although we have adopted most of those Guidelines, we have decided to deviate in respect of how we present the data.

Specifically, ISED suggested enumerating requests only when the number of requests exceed 100; anything below 100 is suggested to be represented by a range of 0-100. While that threshold may make sense for larger telecommunications companies, TekSavvy is still relatively small. We do not receive hundreds of requests from government agencies therefore enumerating requests in a manner consistent with ISED's Guidelines would not provide the level of transparency that we aim to achieve.

Overview

In total, between January 1, 2017 and March 31, 2017, TekSavvy received 29 requests for information from government agencies. Of those requests, we made 22 disclosures in response to those requests, which is representative of a 76% response rate.

In this report, the total number of requests for information from government agencies has been broken down into two main categories: by authority and by jurisdiction.

"Authority" indicates whether or not the government agency making the request has done so in accordance with the law. We have broken down the data by authority to include four different subcategories: at the initiative of the organization, informal, court ordered, and emergency (sometimes called "exigent").

"Jurisdiction" indicates what level of government the requests came from. We have broken down the data by jurisdiction to include three subcategories: provincial and municipal, federal, and non-Canadian.

The data contained in each subcategory is enumerated by the number of requests of each type we received, and the numbers of those requests that we answered with disclosures or rejections.

Following this data in the table below, we examine our disclosure policies and practices to provide an in-depth explanation of the data.

By Authority				
	Type of Request	**Number of Requests**	**Number of Disclosures**	**Number Rejected**
1	At the Initiative of the Organization	N/A	1	N/A
2	Informal	~7	0	All (~7)
3	Court Ordered	19	17	0
4	Exigent or Emergency	3	3	0
By Jurisdiction				
	Type of Request	**Number of Requests**	**Number of Disclosures**	**Number Rejected**
5	Provincial Government Agencies	20	13	7
6	Federal Government Agencies	9	7	0
7	Foreign Government Agencies	0	0	0

By Authority

1) Disclosures Made at the Initiative of the Organization

During this reporting period,
TekSavvy made one disclosure at our own initiative.

This category is used to describe any disclosures TekSavvy made proactively. This number is extremely low because we only make voluntary disclosures if TekSavvy becomes aware of a real and imminent threat being made to someone's wellbeing. These kinds of circumstances do not occur often. When they do, they typically result from one of our agents overhearing physical violence during a phone interaction with our customers.

TekSavvy Policy

We record all of our phone conversations with our customers. These recordings are retained for a period of two years to assist in the resolution of service-related or billing disputes.

2) Informal Requests

Of the 29 requests received during this reporting period,
approximately seven were informal requests.
TekSavvy made no disclosures is response to those requests.

Informal requests are requests that lack legal authority. This means that the agency making the request is not doing so under any law – they are simply asking for us to voluntarily provide them with the requested information.

The most common kind of informal request received by TekSavvy during the relevant period were jurisdiction requests. A jurisdiction request is a document prepared by a law enforcement agent that is intended to gather information about the location of a subscriber. Jurisdiction requests are not court orders. Since we are not required to disclose information in response to a jurisdiction request, our policy is not to disclose any information.

Note that it is difficult for us to know the exact number of these requests. We say that we received "approximately" that many informal requests because these requests sometimes also come in the form of a phone call or email which are comparatively difficult for TekSavvy's Data Protection Office to log and track.

TekSavvy Policy

While Canada's private sector privacy law (PIPEDA) may allow organizations to voluntarily disclose the personal information of a subscriber in certain circumstances, TekSavvy has opted to only make voluntary disclosures in emergency circumstances.

After disclosure of a subscriber's personal information has been made to a government agency, we notify the individual of the disclosure unless, of course, we are prohibited from doing so by law.

3) Court Ordered Requests

Of the requests received during this reporting period,
19 were court ordered requests.
TekSavvy made 17 disclosures in response to those requests.

This category describes any requests for information from government agencies made pursuant to a court order. The most common kind of court orders received by TekSavvy during the relevant period were "Production Orders" pursuant to section 487.014 of the *Criminal Code.*

The disclosure percentage in this particular subcategory is very high at 89.5% because TekSavvy is legally required to comply with court orders. This is true insofar as the court order is compliant with the relevant legislation and is not overreaching or overbroad.

In the event that we are served with a court order that omits required information, is formatted incorrectly, is overreaching, or overbroad, we make our best attempts to work with the agency requesting the information to reach a mutual understanding and appropriately address any issues. Though we reserve our right to challenge a court order, we did not exercise that right with respect to any of the requests we received during the period of January 1, 2017 to March 31, 2017.

The discrepancy between the number of court ordered requests we received and the number of disclosures made in response to those requests can be attributed to orders that sought information TekSavvy did not have. In those circumstances, we advise the agency that made the request only that we do not have the relevant information.

TekSavvy Policy

TekSavvy only retains information that correlates a subscriber with an electronic address (IP address) for a period of 30 days after that IP address is no longer associated with that specific subscriber. This policy is consistent with PIPEDA's requirement for organizations to keep personal information belonging to its subscribers for no longer than required in the ordinary course of business.

4) Emergency (Exigent) Requests

**Of the requests received during this reporting period,
three were requests for information in relation to exigent or
emergency circumstances.
TekSavvy made three disclosures in response to those requests.**

This category includes all requests made in relation to "*an emergency that threatens the life, health or security of an individual*" as set out in subsection 7(3)(e) of *PIPEDA* which allows organizations such as TekSavvy to disclose a subscriber's personal information without their knowledge or consent.

TekSavvy Policy

Before disclosing information in response to an emergency or exigent request, TekSavvy requires the party making the request to answer a series of questions intended to establish the urgency of the request and the importance of the requested information. This approach ensures compliance with subsection 7(3)(e) of PIPEDA as it requires the requesting party to demonstrate a threat to the "life, health or security of an individual" before we disclose the requested information.

For additional information regarding how TekSavvy responds to requests made in emergency or exigent circumstances, please refer to our Law Enforcement Guide.

By Jurisdiction

5) Provincial & Municipal Government Agencies

Of the requests received during this reporting period, 20 were requests for subscriber information from provincial government agencies.
TekSavvy made 12 disclosures in response to those requests.

The percentage of requests that resulted in disclosure in this particular subcategory is relatively low with just a 65% disclosure rate. This low disclosure rate can be partially attributed to the fact that all seven jurisdiction requests that we received during the relevant period came from either a municipal or provincial government agency. As previously mentioned, we do not make disclosures in response to jurisdiction requests.

One request from a municipal or provincial government agency yielded no relevant information, so no disclosure was made.

6) Federal Government Agencies

Of the requests received during this reporting period, nine were requests for information from federal government agencies.
TekSavvy made seven disclosures in response to those requests.

Federal agencies have met with TekSavvy to discuss practices on both sides that respect investigative needs while protecting subscriber privacy. As a result, their requests for information are relatively likely to result in disclosures. For instance, in our experience, federal agencies generally no longer use jurisdiction requests. As a result, the disclosure rate for this subcategory is fairly high at 77.8%.

Two requests from federal government agencies yielded no relevant information, so no disclosures were made.

7) Non-Canadian Government Agencies

During the relevant period, TekSavvy did not receive any requests for information from non-Canadian government agencies.

TekSavvy Policy

It is TekSavvy's policy not to disclose subscriber information unless we are required to do so. Non-Canadian government agencies do not have authority to directly require us to disclose information to them. Instead, they can make use of a Mutual Legal Assistance Treaty (MLAT), which is a legal instrument (see the *Mutual Legal Assistance in Criminal Matters Act)* to facilitate the cooperation of a foreign law enforcement agency and a Canadian law enforcement agency to ensure the request for information is compliant with Canadian law.

Types of Information Requested

The ISED Transparency Reporting Guidelines previously referred to in this report suggest breaking down requests by types of information sought. There were 5 suggested categories: basic identifying information, tracking data, transmission data, stored data and real-time interception.

Basic identifying information is any personal identifier and may include data points such as a subscriber's name, service address, billing address, telephone number or email address. All but one of the 29 requests received during the period of January 1, 2017 to March 31, 2017 requested basic identifying information.

Tracking data is defined by ISED as data that relates to the location of a transaction, individual or thing. Within this meaning of tracking data, all but one of the requests received during the relevant period were for tracking data.

Transmission data may include the MAC address of a cable internet modem, the login of a DSL modem and any other modem identifiers such as the make, model, and serial number of the device. Of 19 court ordered requests for information received during the relevant period, four included requests for transmission data.

Stored data is any information that is collected and then kept for any period of time. All of the requests received during the relevant period were for stored data.

Real-time interception occurs when communications are intercepted as they occur, typically through the means of a wiretap. To date, TekSavvy has not been asked to take part in the real-time interception of its subscribers' communications.

For an in depth examination of what types of information TekSavvy collects and retains about its subscribers, and for more information about our privacy practices, please refer to our Privacy Policy, and our Privacy FAQs, our Law Enforcement Guide, and our response to CitizenLab's 2017 request for information about our privacy and transparency practices.