TekSavvy Solutions Inc.

Law Enforcement Guide

TekSavvy Solutions Inc. is a provider of Internet access, voice telephony, and related telecommunication services. Hastings Cable Vision Ltd. is a broadcast distribution undertaking, Internet and voice service provider, and an affiliate of TekSavvy Solutions Inc. This document refers to both companies together as the TekSavvy Companies, or simply as "TekSavvy".

We retain subscriber information in accordance with our Privacy Policy and Terms of Service. As innovators in the protection of online consumer rights, we are committed to protecting the privacy of our customers.

The purpose of this Guide is to assist law enforcement agencies in understanding TekSavvy's retention and disclosure practices. That being said, these practices are subject to change without notice.

Table of Contents

1 Quick facts

- **Privacy:** TekSavvy will not disclose personal information to third parties unless we are required to by law, such as by a Production Order or other court order. This includes the existence of IP correlation information or the jurisdiction of a particular end-user.
- **Email address for Preservation Demands and Production Orders: tsiprivacy@teksavvy.com**
- **Phone number for emergency requests only: 1-613-518-7803.** Please call only where the life, health, or security of an individual is threatened and the conditions for a Production Order are present, but emergency (*i.e.* "exigent") circumstances prevent one from being obtained. More information is provided below about our process to confirm that these conditions are present.
- **Retention period:** TekSavvy stores information that can be used to identify the end-user who was assigned a given IP address at a given time. That information is retained for as long as the session is open and the IP address is associated with that user, and then for 30 days after the session ends and the IP address is no longer associated with the user. The retention period for Hastings Internet customers in Madoc, Ontario may be different.
- **Informing end-users:** TekSavvy notifies individuals of third-party requests regarding their TekSavvy accounts unless we are legally prohibited from doing so. This includes disclosing Preservation Demands, Production Orders, and disclosures in emergency circumstances to the affected end-users.
- **Aggregated reporting:** For the purpose of public accountability, TekSavvy regularly releases a transparency report that aggregates the number of requests received by category without disclosing details of those requests.

2 General Information

TekSavvy is a provider of Internet access, voice telephony, and related telecommunication services. We retain subscriber information in accordance with our Privacy Policy and Terms of Service. As innovators in the protection of online consumer rights, we are committed to protecting the privacy of our customers. This guide is designed to assist law enforcement in understanding TekSavvy's retention and disclosure of information practices, which are subject to change without notice.

Consistent with sub-paragraph 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), TekSavvy will produce information where that disclosure is (a) pursuant to a lawful authority; (b) in the context of a law enforcement investigation; and (c) restricted to basic subscriber information. Further, we will only make such disclosures in response to a Canadian Production Order, or in instances in which the conditions for such an order or warrant were present but exigent circumstances prevented one from being obtained (see 6. Emergency Requests for Information).

TekSavvy's approach to law enforcement requests is consistent with, and remains unchanged following the recent Supreme Court decision in *R v. Spencer*, 2014 SCC 43, where the court found that a request to link an IP address with subscriber information can in effect be a request to link a specific person to specific online activities.

3 Subscriber Information

We typically receive requests to correlate Internet Protocol ("IP") addresses with a subscriber's name, service address (or sometimes "physical" address), and telephone number. Most of this Guide is about requests where a law enforcement agency has an IP address and is seeking to identify the subscriber associated with that address at a specific date and time.

As a provider of voice services, TekSavvy also receives requests to identify the subscriber associated with a phone number, or to disclose records about calls. Please see the section in this Guide about Phone Records for more information about those records.

3.1 IP Address Information

The ARIN Whols database (http://whois.arin.net) provides publicly available information about whether or not an IP address belongs to TekSavvy.

Please note that it is difficult to accurately correlate an IP address with a geographic location. While there are publicly available third-party services that attempt to locate an IP address to a geographical location, this information may be inaccurate. That being said, in our experience, these sources of information are often a useful guide to the geographic area where an IP address may be located.

TekSavvy logs different information about IP addresses on different technological infrastructures in various locations. For Fibre, Fixed Wireless, and DSL-based access, we log IP addresses assigned directly to user accounts. For cable-based access, we log IP addresses assigned to devices' MAC addresses through which we, in turn, link the IP address to the associated user account. When we log IP address allocation information, we retain the times and dates when an IP address began to be used (when it was "leased"), and when the lease expired.

In the ordinary course of TekSavvy's business, the longest IP address records are required to be retained is 30 days after they cease to be associated to the subscriber. TekSavvy purges IP address records from our logs when we no longer need to retain them, which is therefore 30 days after they cease to be associated to the subscriber. Note that the retention period for Hastings Internet customers in Madoc, Ontario may be different.

In practice, that means that TekSavvy may still have information today about an IP address lease on a date more than 30 days in the past if that IP address lease continued to be open until a date within 30 days before today. Once the session ends and the IP address lease expires, we continue to retain both the start and end dates for that session, until we finally delete all information about that session, 30 days after the lease expires.

As more Internet service providers and more Internet services adopt IPv6 addresses, TekSavvy has seen more court orders seeking to identify subscribers from IPv6 addresses. Some TekSavvy subscribers have IPv6 addresses, so it is important to understand how those addresses work in order to seek the right information from us.

First, some definitions:

Term	Definition
“IPv6 address”	A 128-bit alphanumeric value that identifies an endpoint device in an Internet Protocol Version 6 (IPv6) network. IPv6 addresses consist of eight groups of 16-bit hexadecimal values separated by colons (:) and are generally composed of two parts: the network prefix and the interface ID.
“Routing prefix”	The first three groupings or the first 48 bits in an IPv6 address.
“Subnet ID”	The fourth grouping, bits 49 to 64 in an IPv6 address.
“Network prefix”	The routing prefix and subnet ID together, make up the leading 64-bit network prefix in an IPv6 address. The network prefix remains constant for every device connected within the subscriber’s network.
“Interface ID”	A unique identifier assigned by the subscriber’s equipment to each device connected within its network. The interface ID consists of the last four groupings or the last 64 bits in an IPv6 address.
“IPv6 text representation”	The recommendation for canonical text representation format of IPv6 addresses presented by the Internet Engineering Task Force (IETF).

IPv6 addresses are allocated to TekSavvy subscribers in the following manner:

a) TekSavvy’s underlying network access service provider assigns the leading 64-bit network prefix of an IPv6 address to a subscriber which is delegated by the subscriber’s equipment to all devices connected within its network. Please note that the same network prefix cannot be assigned to more than one subscriber at a time.
b) The subscriber’s equipment assigns to each individual device connected within its network, a unique interface ID which makes up the last 64 bits in an IPv6 address.

TekSavvy does not have visibility into or information about the interface ID (the last 64 bits of an address), and neither does our underlying network access service provider. As a result, we are unable to correlate a fully notated 128-bit IPv6 address.

In short, if you know an IPv6 address and you are seeking to identify the associated TekSavvy subscriber who was using that address, if TekSavvy has associated logs then TekSavvy would identify the subscriber based on only the network prefix, being the first 64 bits, or 4 groupings. We will not have any information about the fully notated IPv6 address or the specific equipment or interface the subscriber used on that address.

3.2 Subscriber Information that TekSavvy does not retain, and cannot provide

3.2.1 Unless there are exigent circumstances, TekSavvy will not disclose information without a court order

TekSavvy does not provide customer-specific information to law enforcement without a court order. This includes:

- information about the existence or non-existence of records relating to a specific IP address;
- information relating to the geographical location or "jurisdiction" of a subscriber's service; and
- any other customer-specific information.

After receiving a Production Order, Preservation Demand, or other court order, we look up information as soon as reasonably possible. When we receive a Preservation Demand, we preserve the requested information, including in particular the information correlating an IP address with an end-user's account. If no such information is found—either because no information was logged or because the retention period expired—we endeavour to advise the officer who made the request without delay.

3.2.2 Information about what our subscribers do online, or how they use their Internet service

We do not log any information, such as IP addresses, domain names, or port numbers of sites, services, or protocols that are visited or used by subscribers. Since we currently do not have a business need to track or collect this information, we simply do not track or collect it.

3.3 Telephone Service Information

TekSavvy currently provides two voice calling services, both of them interconnected with the Public Switched Telephone Network. The first, TekTalk, is a managed Voice over Internet Protocol service, otherwise known as VoIP. The second, Home Phone, is a resold landline phone service of an Incumbent Local Exchange Carrier ("ILEC").

TekSavvy does not currently offer mobile wireless services and therefore, we do not have records of text ("SMS") or multimedia ("MMS") messages and do not have GPS or cell tower information, nor do we undertake targeted geolocation of devices.

3.3.1 Call Detail Records

Call detail records ("CDRs") are call-level metadata records maintained in respect of voice telephony services. Any call detail record 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.

For TekTalk service, call detail records generally consist of the following data points; Caller Number, Called Number, Call Type (Outgoing or Incoming), Date and Time Call Initiated, Date and Time Call Connected, Date and Time Call Ended, and Call Duration.

For Home Phone long distance service, outgoing call detail records generally include, Caller Number, Called Number, Date and Time of Call, Call Duration, and Call Destination (City).

TekTalk generates CDRs for all incoming and outgoing calls, both local and long distance.

For Home Phone, the underlying ILEC provides to TekSavvy details about outgoing long-distance CDRs, which TekSavvy retains for account and billing purposes.

The ILEC does not collect, store, or provide to TekSavvy any incoming long-distance CDRs or any local (incoming or outgoing) call records.

3.3.2 Subscriber Records

For TekTalk and Home Phone, TekSavvy understands the term "subscriber information" to mean the subscriber's name, telephone number and installed service address.

TekSavvy may correct, update or complete subscriber information if the records are inaccurate or incomplete. In rare circumstances, subscriber records may be purged upon request or if we no longer have a business purpose for retaining this information.

TekSavvy does not collect or store subscriber name or address records for telephone numbers which are not assigned to TekSavvy telephone subscribers regardless of who they are calling.

For TekTalk, we collect, and store telephone number records of incoming local and long-distance calls made to TekTalk subscribers.

4 Requests for Preservation of Data

4.1 Who to Contact

Preservation Demands, Preservation Orders, and related inquiries can be sent:

via e-mail to:	tsiprivacy@teksavvy.com
via mail to:	Data Protection Office TekSavvy Solutions Inc. 800 Richmond Street Chatham, Ontario N7M 5J5

4.2 Preservation Demands

Demands to preserve computer data pursuant to subsection 487.012 of the *Criminal Code* must be in Form 5.001 (Subsection 487.012(1) – See Attachment A below). Please note the following:

- The form must be addressed to the following address:
  - "TekSavvy Solutions Inc." of "800 Richmond Street, Chatham, Ontario, N7M 5J5".
- TekSavvy Solutions Inc. is, at law, a legal person that controls and possesses subscriber data. If the form is instead addressed to an individual, since that individual does not possess any subscriber data, we may not be able to locate any information in response to your Preservation Demand.
- The form must **specify** the data to be preserved. If this includes data relating to an IP address, it must include the relevant date and time when the IP address was in use.
- Pursuant to subsection 487.012 of the *Criminal Code*, Preservation Demands automatically expire after either
  a) 21 days if it relates to an offence under any act of Parliament or
  b) 90 days if it relates to an offence committed under a law of a foreign state.

  The date on Form 5.001 must reflect the appropriate one of those two periods of time. Other periods of time are not valid on a Preservation Demand.
- The form must be complete and include the requesting officer's name and signature.

Data that is not otherwise kept in the normal course of business during the period to which the Preservation Demand relates will be destroyed following the expiry of the Preservation Demand.

4.3 Preservation Orders

Preservation Orders to preserve computer data pursuant to 487.013 of the *Criminal Code* must be in Form 5.003 (Subsection 487.013(4) – See Attachment B below). In accordance with the law, TekSavvy will preserve, but not disclose, a one-time data pull of the requested existing subscriber data available at the time the Preservation Order is received, for a period of 90 days, unless revoked earlier.

4.4 Disclosure of Preservation Demands and Preservation Orders to Relevant Individuals

Preservation Demands and Orders are "personal information" within the meaning of subsection 2(1) of PIPEDA. As a result, we notify individuals of third-party requests regarding their TekSavvy accounts unless we are legally prohibited from doing so.

Upon expiry of the Demand or Order, a notification letter disclosing the Preservation Demand or Order is sent to the relevant individual and all preserved data are destroyed.

In the event the Preservation Demand or Order is followed by a Production Order, we will withhold disclosure of the Preservation Demand or Order to the relevant individual until after we have responded to the Production Order and any associated Non-Disclosure Order has expired.

5 Requests for Disclosure of TekSavvy Subscriber Information

5.1 Who to Contact

Court orders requesting subscriber information and related inquiries can be sent:

via e-mail to:	tsiprivacy@teksavvy.com
via mail to:	Data Protection Office TekSavvy Solutions Inc. 800 Richmond Street Chatham, Ontario N7M 5J5

5.2 A Production Order is Generally More Appropriate than a Warrant

Production Orders require us to disclose information that we have: Nearly all lawful requests for subscriber information received by TekSavvy are accompanied by a General Production Order under section 487.014 of the *Criminal Code*. A Production Order requires the custodian of documents or data (TekSavvy) to deliver or make available the documents or data to persons such as law enforcement officials within a specified period of time. When TekSavvy receives a valid Production Order, we complete a search of our own systems and provide the results of the search to the requesting law enforcement official(s).

Warrants authorize a law enforcement agency to search for evidence: We receive warrants more rarely than we receive Production Orders. A warrant gives a law enforcement agency the permission to enter private property (such as the TekSavvy offices) and to search for evidence. A warrant requires nothing of TekSavvy except that we not interfere with law enforcement entering the premises to search for things named in the warrant. As such, TekSavvy will not complete a search of its own systems in response to a warrant.

5.3 Production Orders

TekSavvy requires the following with respect to Production Orders:

- **Who is named in the Order:** The Production Order should be addressed to the following address:
  - "TekSavvy Solutions Inc." of "800 Richmond Street, Chatham, Ontario, N7M 5J5".

  The Production Order must not be written out to an individual employee. TekSavvy Solutions Inc. (or in rare cases, Hastings Cable Vision Ltd.) is, at law, a person that controls and possesses subscriber data.

  That being said, we understand that some Justices and Judges apparently prefer for orders to be directed to individuals. While current law does not require that an individual be named, in circumstances where a Justice or Judge prefers or requires that an individual's name appears on an order, we would suggest that the order be directed to the individual member of TekSavvy's Data Protection Office "or a designate" (*e.g.* "Joan Smith or a designate"). That phrase allows the

individual to name the appropriate TekSavvy company as the designate who may have possession or control of the relevant documents or data. Please contact us for an appropriate individual to name.

- **What information is to be disclosed:** The order must **specify in detail** the data that is to be produced. If this includes data relating to an IP address, it must include the relevant **date and time** that the IP address was in use. No more personal information should be requested than is required for the purpose of the order, especially as we will inform any named individuals except where we are not permitted to do so (see 5.6 *Disclosure of Orders to Relevant Individuals*).

  The following text is our most common form of request, which we find to be clear and unambiguous:

  > "The subscriber name, physical address, and phone number associated to the IP address ###.###.###.### on January 1, 2023 at 13:50:00 UTC."

  Other phrases in your request may or may not be clear to us, and may not result in us disclosing the information that was intended in the request. We recommend requesting just the information you need, and describing it clearly:

  - **Example 1:** "name, physical address, and phone number": This clearly spells out exactly the information that is required for the purpose of the order, and is likely sufficient information for most investigations.

  - **Example 2:** "subscriber information": We understand this to mean only the end-user's name, telephone number, and the physical address where service is delivered.

  - **Example 3:** "all information": This is generally too broad and results in unnecessary work for both TekSavvy and the investigating officers. Such requests may produce a great deal of irrelevant administrative information.

  - **Example 4:** "payment information": Since credit card details are sensitive personal financial information, our expectation is that the Judge or Justice ordering the disclosure would clearly specify in the order that such detailed financial identifiers were required. In the absence of specifically requiring the disclosure of credit card details, we understand the phrase "payment information" to mean the method used to make payments, generally (credit card, due upon receipt, etc.), as well as the dates and dollar amounts of payments relevant to the time period provided in the order or demand .

  - **Example 5:** "account history": It is not clear what specific data this phrase refers to; we may not be able to provide any relevant data.

- **Who made the order:** The order must be signed by a Justice of the Peace or Judge. The name of the Justice of the Peace or Judge should be provided separately at the time the order is submitted to TekSavvy or written clearly on the order.

- **Time provided to produce requested documents:** We fill requests within the allotted time period and sooner where resources permit. The management of law enforcement requests for information is not automated and therefore requires considerable effort on our part. Most requests allow us **30 days** to complete our response.

- **Attachments:** In the past, many Production Orders we received would provide the details about the requested information in an attachment or appendix to the order. Sometimes, that attachment or appendix would be formatted and written as though it were its own Production Order. This was a confusing approach that complicated the Production Order itself, especially if there were discrepancies between the Production Order and the attachment or appendix. While this has not been an issue in recent years, we still advise law enforcement agents to help avoid these complications by limiting any attachments, and avoiding attachments that are structured as Production Orders.

- **Who our response is sent to:** A Production Order specifies who the information should be sent to. Since most Production Orders we receive are accompanied by Non-Disclosure Orders, we are not able to disclose our response to anyone—including other law enforcement officials—other than the person named in the Production Order at the email or physical address provided in the order. If you are going to be unable to receive our response and would like the information to be disclosed to another individual, you would need to apply to the court to amend the order. Alternatively, if you provide the contact information for the other individual, TekSavvy will let them know when the information has been sent, and they can use internal processes to access that response.

5.4 Non-Disclosure Orders

Where non-disclosure of a Preservation Demand or a Production Order is sought, TekSavvy requires the submission of a Non-Disclosure Order in Form 5.0091 (Subsection 487.0191(3) – See Attachment C below).

Because the *Criminal Code* specifically provides the Non-Disclosure Order as a mechanism to prevent disclosure of a Production Order, non-disclosure requirements should not be part of the conditions attached to a Production Order, which are provided for in section 487.019. Instead, we follow the explicit non-disclosure requirements provided for in section 487.0191, and we reserve our right to challenge a Production Order with a disclosure condition. As such, if disclosure is to be restricted, we advise law enforcement to apply for a Non-Disclosure Order using Form 5.0091.

5.5 International Requests

TekSavvy will not release information in response to requests from non-Canadian law enforcement agencies. In order to obtain information, non-Canadian law enforcement agencies must work with a

Canadian law enforcement agency through a Mutual Legal Assistance Treaty (MLAT) and submit a Production Order issued by a Canadian court.

5.6 Disclosure of Orders to Relevant Individuals

Production Orders, and our responses to them, are "personal information" within the meaning of subsection 2(1) of PIPEDA. We are generally required to inform individuals when we disclose their information to a third party. As a result, we notify individuals of third-party requests regarding their TekSavvy accounts unless we are legally prohibited from doing so.

Following disclosure to a third party, a notification letter is sent to the relevant individual. This notification includes a copy of the submitted orders, the date of disclosure, reasons for disclosure, and substance of the disclosure. These documents are password protected to ensure added privacy protection.

TekSavvy will disclose Production Orders and our response to them to the relevant individuals except where:

a) We receive a Non-Disclosure Order in Form 5.0091 (Subsection 487.0191(3) – See Attachment C below) that explicitly prohibits disclosure of the existence, contents, or any of the portion or portions of the Production Order. TekSavvy will abide by Non-Disclosure Orders, but if the non-disclosure prohibition is of an indeterminate length, **we will re-contact the third party in the future to determine whether it is still necessary and in effect.**

b) Disclosure could reasonably be expected to be injurious to

   i. national security, the defence of Canada or the conduct of international affairs;

   ii. the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or

   iii. the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

If disclosure to the relevant individual would be injurious to one of the above, and as a result the officer or agency objects to us informing the affected individual of the Production Order (or other request for information) and our response to it, then we ask law enforcement to provide us with a Non-Disclosure Order that prevents us from informing the end-user for a specified period of time. If it is not possible to seek or obtain a Non-Disclosure Order, we ask that the officer inform us of the circumstance and the date on which the information can be disclosed. Depending on the objection and the circumstances, we either seek clarification from the court or look to sections 9(2.1) to (2.4) of PIPEDA for guidance, informing the Office of the Privacy Commissioner if appropriate.

5.7 Aggregation of Request Data into Statistical Reporting

For the purpose of public accountability, TekSavvy is implementing regular transparency reporting. This quarterly report aggregates the number of requests we received by category, and does not disclose the particular circumstances, contents, or specific parties involved in any law enforcement demand or judicial

order. Reporting in this manner does not inform any third party of the content or the existence of any such demand or order. Looking at all of the requests we receive each quarter, we aggregate information about those requests and our responses to them. We publish the report after at least six months has passed from our last response to any of those requests. This complies with guidelines published by Innovation, Science, and Economic Development Canada (ISED).

6 Emergency Requests for Information

In accordance with section 3.1 of the TekSavvy Privacy Policy, TekSavvy may disclose personal information to a requesting Canadian law enforcement agency where the life, health, or security of an individual is threatened and the conditions for a Production Order are present but exigent circumstances prevent one from being obtained. For example, this may apply to requests regarding a hostage situation, missing minor, bomb threat, shooting threat, or suicide threat.

6.1 Who to Contact

To make an emergency request where the life, health, or security of an individual is under **immediate threat**, please notify us by calling: **1-613-518-7803**

6.2 How to Make an Emergency Request for Information

First, to make sure that your request is received and actioned as soon as possible, please phone **1-613-518-7803.** Even if you are familiar with our process and you send a completed request form first, please phone to make sure our team receives the email without delay.

TekSavvy is not able to disclose personal information without a Production Order, unless the requesting parties have represented that they have reasonable grounds to suspect that the information they are seeking is **needed to prevent bodily harm or death to some person**.

In order to make an emergency request for information, we require the information found at **Attachment D** below to be sent **in writing** to tsiprivacy@teksavvy.com.

Upon receipt, TekSavvy will review the submitted information and evaluate whether the disclosure of an individual's personal information is reasonably required in order to prevent bodily harm or death, whether the circumstances are present to obtain a court order, and whether it is reasonably impracticable to obtain a court order.

Upon reviewing the submitted information, TekSavvy may follow up with the requesting party for further information.

If satisfied that TekSavvy can disclose the personal information, it will be saved in an encrypted PDF file and emailed to the requesting officer. A member of TekSavvy's Data Protection Office will then phone the officer with the password to open the file.

6.3 Disclosure of Emergency Request to Affected Individual

We notify individuals of third-party requests for subscriber information unless we are legally prohibited from doing so. In every case where TekSavvy discloses personal information in response to an emergency request, we will follow up with law enforcement to determine the timing of the disclosure to the affected individual.

6.4 Legal View of Emergency Requests

Our general process: We provide law enforcement with information in emergencies only in accordance with section 487.11 of the *Criminal Code* which permits disclosure of information in exigent circumstances where a warrant or Production Order would have been granted, but there was insufficient time to obtain one. TekSavvy's exigent circumstances questionnaire, provided in Attachment D, helps ascertain whether those circumstances are in place, and provides an accountability trail which we can pursue by returning the form to the agent's chain of command. To proceed with a request in exigent circumstances, we require the requesting officer to complete that questionnaire, and we consider the responses before proceeding.

Emergency circumstances and the Criminal Code: The discussion of exigent circumstances in section 487.11 of the *Criminal Code* relates to warrants, not Production Orders. There is some confusion on this point; both instruments have been used by the courts to compel basic subscriber information from telecommunications service providers. Our understanding is that we are no less compelled by section 487.11 by its focus on warrants, knowing that no equivalent provision exists with respect to Production Orders. Our understanding is informed by the discussion of exigent circumstances in *R. v. Spencer*, whose facts and circumstances—the obtaining of basic subscriber information, from an Internet service provider, by law enforcement, in respect of a child pornography offence—are very much on point.

Disclosure of information, and PIPEDA: Because we are compelled by section 487.11 to provide information in exigent circumstances to law enforcement, there is no conflict with PIPEDA. Paragraph 7(3)(c.1) of PIPEDA is the authorizing provision, and section 487.11 of the *Criminal Code* is the compulsion that is required to meet the "lawful authority" requirement.

Informing end-users, and PIPEDA: Paragraph 7(3)(c.1) of PIPEDA does not compel us to inform the account holder of the third-party disclosure in these circumstances. However, where it does not jeopardize public safety, informing an end-user that their information was provided to a third party is always the best approach, and our practice is to do so.

If the requesting officer objects to us informing the end-user: First responders, like the police, are experts in matters of public safety. Especially where the first responder is the third party in question, we must seek out their view and consider it prior to disclosure. If their view is that disclosure is not appropriate, and their view is reasonable, then we must note this, avoid disclosure, but follow up regularly in writing to understand whether this view has changed and, if not, why. At the same time, since it is our practice to inform end-users of all disclosures to third parties, in the event the requesting authority continues to object to us informing the individual but no court order prevents us from doing so, we look to sections 9(2.1) to (2.4) of PIPEDA for guidance, and we inform the Office of the Privacy Commissioner of Canada.

6.5 Suicide Prevention Practices

TekSavvy receives a high volume of calls at all hours. Very rarely, TekSavvy's customer service and technical support agents handle calls from people who threaten self-harm or present a material risk of suicidal activity. In such cases, our agents may help the caller transfer to a crisis line or, if there is a real and imminent threat, to emergency services. In extreme circumstances, where it appears to our agent

that the caller has both a desire and intent to die and the capability of carrying out that intent, TekSavvy may dispatch local police as the designated first responders.

7 FAQ

1. **Where can I send my request and related inquiries?**
    a. If you are making a request regarding an emergency where the life, health, or security of an individual is under immediate threat, please notify us be **calling 1-613-518-7803**.

    b. Otherwise,

via e-mail to:	tsiprivacy@teksavvy.com
via mail to:	Data Protection Office TekSavvy Solutions Inc. 800 Richmond Street Chatham, Ontario N7M 5J5

2. **How will I know TekSavvy received my emailed request?**
    a. We will confirm receipt via reply email.

3. **When will the response be ready?**
    a. We fill requests within the allotted time period and sooner where resources permit. Management of law enforcement requests for information is not automated and therefore requires considerable effort on our part. Most requests allow us 30 days to complete our response.

4. **The order I submitted is regarding the investigation of a very serious crime. Will TekSavvy prioritize it over other orders?**
    a. We have to respect the deadlines of all judicial orders and we are legally obligated to fill them by the stated dates. This means we cannot default on answering an order regarding a less serious crime in order to more quickly answer an order regarding a more serious crime.

5. **Does TekSavvy have a lot of other law enforcement requests?**
    a. We receive a regular volume of requests and devote a considerable amount of time to filing these. Please note that we are generally prohibited from disclosing the existence of specific judicial orders, and we cannot provide detailed information about the types and amount of requests we are processing at any given time. However, we do publish regular transparency reports with aggregated information about requests and disclosures from at least six months ago.

6. **Does TekSavvy notify the relevant individual of any disclosure to law enforcement?**
    a. We notify individuals of third-party requests regarding their TekSavvy accounts unless we are legally prohibited from doing so (see 5.6 Disclosure of Orders to Relevant Individuals).

7. **I understand TekSavvy won't disclose customer-specific information without a court order. Will you confirm whether or not you have the records I am seeking?**
    a. We can advise of our general practice, which is to delete records of IP addresses on a rolling basis 30 days after each address is no longer associated with a subscriber. The retention period for Hastings Internet customers in Madoc, Ontario may be different. We will not undertake a lookup of records relating to a particular IP address without a court order or a Preservation Demand.

8. **Why does TekSavvy delete IP address records after 30 days?**
    a. We strive to retain only as much personal information as is necessary to provide our services to our customers. Since we bill customers on a monthly basis, we only require such records for 30 days. It is therefore TekSavvy's practice to purge IP address records after 30 days, because at that point they are no longer required in the ordinary course of business.

9. **I am requesting records relating to a specific IP address. Why does TekSavvy require the date and time the IP address was in use?**
    a. The date and time are integral to a request regarding a specific IP address because IP addresses are generally leased to subscribers temporarily. For example, the same IP address can be leased to one person at 10:00 a.m. and another person at 10:03 a.m. This means it is possible for a very large group of people to use the same IP address within a single day.
    b. It is very important that you specify the time zone of the time for which you are requesting the IP address information. Our logs may record different time zones, however we generally receive requests in GMT/UTC. The time zone is required to ensure we correlate the correct end-user.

10. **If my Preservation Demand expires before my investigation is complete, will you retain the preserved data for an extended period of time?**

    No. Section 487.0194 of the *Criminal Code* requires that computer data preserved in response to a Preservation Demand that would not be retained in the ordinary course of business be destroyed as soon as feasible after the demand expires or is revoked.

11. **Are you able to provide:**
    a. Host computer names?
        i. We don't capture computer hostnames and therefore cannot provide them.
        ii. In some cases, we do retain the MAC address of a device plugged directly into the first LAN port of the modem.

    b. Modem identifiers?
        i. We sometimes retain information about customer modems, including the make and model, MAC address, and modem serial numbers, but this can vary depending on whether or not the customer uses a TekSavvy-issued modem.

c. Email passwords?

i. No. TekSavvy does retain records relating to TekSavvy email passwords, but these are encrypted and we cannot decrypt them.

d. Information about what websites subscribers visited?

i. We do not log any information about sites, services, or protocols that are visited or used by subscribers, including IP addresses, domain names, or port numbers. Since we currently do not have a business need to track or collect this information, we simply do not track or collect it.

e. Payment information?

i. TekSavvy retains records about the frequency of payment, method of payment, and other details about account billing and payment. Because TekSavvy provides its services on a prepaid basis, it does not have a business need to conduct credit checks on its subscribers nor does it have information relating to its subscribers banking as it does not offer automatic withdrawal as a payment method.

ii. Since credit card details are sensitive personal financial information, our expectation is that the Judge or Justice ordering the disclosure would clearly specify in the order that such detailed financial identifiers were required. In the absence of specifically requiring the disclosure of credit card details, we understand the phrase "payment information" to mean the method used to make payments, generally (credit card, due upon receipt, etc.), as well as the dates and dollar amounts of payments relevant to the time period provided in the order or demand. If you are asking a court to order disclosure of payment card details, we recommend incorporating the following text in the list of documents and data to be produced: "Payment card information, specifically the method of payment used, payment card type, payment card number, payment card expiry date and name associated to the payment card."

iii. Note, however that TekSavvy does not collect or store complete payment card numbers and therefore, we cannot produce complete payment card numbers.

iv. Although we do record a name in relation to any payment card identifiers we are provided with, that name may not necessarily be the name as it appears on the payment card to which the identifiers relate.

Attachment A — Preservation Demand Form

FORM 5.001
(Subsection 487.012(1))
PRESERVATION DEMAND

Canada,

Province of .....
(*territorial division*)

To (*name of person*), of .....:

Because I have reasonable grounds to suspect that the computer data specified below is in your possession or control and that that computer data

will assist in the investigation of an offence that has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*),

(*or*)

will assist in the investigation of an offence that has been committed under (*specify the provision of the law of the foreign state*) that is being conducted by a person or authority, (*name of person or authority*), with responsibility in (*specify the name of the foreign state*) for the investigation of such offences,

you are required to preserve (*specify the computer data*) that is in your possession or control when you receive this demand until (*insert date*) unless, before that date, this demand is revoked or a document that contains that data is obtained under a warrant or an order.

This demand is subject to the following conditions:

If you contravene this demand without lawful excuse, you may be subject to a fine.

You are required to destroy the computer data that would not be retained in the ordinary course of business, and any document that is prepared for the purpose of preserving the computer data, in accordance with section 487.0194 of the *Criminal Code*. If you contravene that provision without lawful excuse, you may be subject to a fine, to imprisonment or to both.

.....
(*Signature of peace officer or public officer*)

2014, c. 31, s. 26

Attachment B — Preservation Order Form

FORM 5.003
(*Subsection 487.013(4)*)
PRESERVATION ORDER

Canada,

Province of .....
(*territorial division*)

To (*name of person*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ,

(*a*) that there are reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the* Criminal Code *or other Act of Parliament*) (*or* has been committed under (*specify the provision of the law of the foreign state*)) and that (*specify the computer data*) is in your possession or control and will assist in the investigation of the offence; and

(*b*) that a peace officer or public officer intends to apply or has applied for a warrant or order to obtain a document that contains the computer data (*and, if applicable,* and that (*name of person or authority*) is conducting the investigation and has responsibility for the investigation of such offences in (*insert the name of the foreign state*));

Therefore, you are required to preserve the specified computer data that is in your possession or control when you receive this order until (*insert date*) unless, before that date, this order is revoked or a document that contains that data is obtained under a warrant or an order.

This order is subject to the following conditions:

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

You are required to destroy the computer data that would not be retained in the ordinary course of business, and any document that is prepared for the purpose of preserving the computer data, in accordance with section 487.0194 of the *Criminal Code*. If you contravene that provision without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of peace officer or public officer*)

2014, c. 31, s. 26.

Attachment C — Non-Disclosure Order Form

FORM 5.0091
(*Subsection 487.0191(3)*)
NON-DISCLOSURE ORDER

Canada,

Province of .....
(*territorial division*)

To (*name of person, financial institution or entity*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to believe that the disclosure of the existence (*or* any of the contents or any of the portion or portions, specified in the information,) of (*identify the preservation demand made under section 487.012 of the Criminal Code, the preservation order made under section 487.013 of that Act or the production order made under any of sections 487.014 to 487.018 of that Act, as the case may be*) during (*identify the period*) would jeopardize the conduct of the investigation of the offence to which it relates;

Therefore, you are prohibited from disclosing the existence (*or* any of the contents or any of the following portion or portions) of the demand (*or* the order) during a period of (*identify the period*) after the day on which this order is made.

(*specify portion or portions*)

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

2014, c. 31, s. 26.

Attachment D — Emergency Request Form for TekSavvy

Emergency Request for Information from TekSavvy Solutions Inc.

a. The IP address that you are inquiring about;

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

c. The personal information you are requesting (for example, name and service address associated with the IP address at that date and time);

d. The name of the law enforcement agency making the request;

e. The occurrence number giving rise to the request;

f. A brief description of the nature of the emergency, including a brief explanation of why it is impracticable to obtain a court order;

g. The information that you are requesting and generally how it will assist in avoiding the imminent bodily harm that you are concerned about;

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

i. The name, rank, and contact information for the Officer in Charge of the investigation; and

j. The name, rank, and contact information for the commander of the particular unit or division with a rank of at least Sergeant and whether they are aware of the request being made.

Please send electronically to **tsiprivacy@teksavvy.com**.
If you have not called to advise us of the emergency, please do so at **613-518-7803.**