



# Securing Your Trust

2016 SASKTEL TRANSPARENCY REPORT

**SaskTel** 

# Table of Contents

Requests for Customer Information	1
Table 1: Breakdown of requests in 2016	2
Types of Requests	3
Voluntary disclosures at the request of a government organization	3
Voluntary disclosures on the initiative of the organization	3
Disclosures in emergency or exigent circumstances	3
Disclosures made in compliance with federal or provincial law	3
Court ordered (warranted) disclosures	3
Other	4
Q & A	5
Why does SaskTel disclose customer information?	5
Can I find out if my information has been disclosed to a government agency?	5
Do you notify your customers when police request their personal information?	5
Does SaskTel have a dedicated group for responding to data requests from government agents?	5
Does SaskTel receive money or other forms of compensation in exchange for providing information to government agencies?	5
Does SaskTel have geo-location information that you may have collected about me, my devices, and/or associated with my account?	6
Do you provide metadata or direct access to customer databases?	6
Does SaskTel receive requests for information in civil cases?	6
How often does SaskTel receive requests?	6
What agencies can request customer information from SaskTel?	6



# Requests for Customer Information

As a telecommunications company and broadcaster of TV services, government and police agencies within and outside the province contact SaskTel requesting information about our customers. This report is designed to provide more detail on the number and different types of requests we receive.

Our customers' privacy is important to us, and that is why we issue this report annually. SaskTel is an open and honest company and we believe our customers need to know what kinds of information are, or are not, provided.

On June 30, 2015, Innovation, Science and Economic Development Canada released voluntary Transparency Reporting Guidelines to assist organizations in maintaining the balance between

openness and the sharing of their customers' personal information while respecting the work of law enforcement, national security agencies, and regulatory authorities.

Citizens expect that when they share personal information with SaskTel it will be safe, and will only be shared under specific conditions. We understand this and want to emphasize that we comply with Saskatchewan's privacy laws and take active steps to protect our customers' information. There is a team of people within SaskTel that have a mandate and directive to proactively manage privacy on a day-to-day basis.

Canadian law enforcement, national security agencies, and regulatory authorities rely on the collection of information to enforce the law and protect public safety. Information may be collected in the context of a criminal investigation, a regulatory audit or inspection, to find a lost or injured child, or to protect an individual from an imminent threat to his or her well-being, among other lawful duties.

All requests that SaskTel responds to require, as a pre-requisite, a legal basis for making such a request. For example, many of the requests

we receive are to respond to court orders from law enforcement agencies. In addition, we receive requests from government departments who are authorized by statute to request information to enforce laws such as the *Income Tax Act*. We also assist police services in life-threatening emergency situations or where there is an ongoing investigation concerning child exploitation.

It should be noted that legal, legislative and policy changes impact the number of requests received by SaskTel. An example of this is *R. v. Rogers Communications*, also known as the "Tower Dump" court case. The demand for information is solely due to the number of investigations government and law enforcement agencies conduct.

We do deny requests for customer information. Except for court orders, SaskTel will refuse to provide the information if we believe the request is vague or not supported by statute. As such, all court orders undergo review.

**TABLE 1: BREAK DOWN OF REQUESTS IN 2016**

Data Type	Number of Requests <sup>1</sup>	Number of Disclosures <sup>2</sup>	Number of Requests Rejected or Contested
Voluntary disclosures at the request of a government agency	393	348	45
Voluntary disclosures on the initiative of the organization	0–100	0–100	NA
Disclosures in emergency or exigent circumstances	1,784	1,390	394
Disclosures made in compliance with federal or provincial law	0–100	0–100	0–100
Court ordered (warranted) disclosures	2,377	1,915	462
a) Basic identifying information (court ordered)	0–100	0–100	0–100
b) Tracking data	0–100	0–100	0–100
c) Transmission data	176	110	66
d) Stored communications content and other stored data	995	840	155
e) Real-time interceptions	1,206	965	241
<b>Other requests</b>			
a) Foreign agency requests (court ordered)	0–100	0–100	0–100
b) Preservation demands and orders	0–100	0–100	0–100
<b>Total Requests<sup>3</sup></b>			
	<b>4,554</b>	<b>3,653</b>	<b>901</b>

<sup>1</sup> Full or Partial Information Disclosed. 0–100 or exact number if over 100

<sup>2</sup> Full or Partial Information Disclosed. 0–100 or exact number if over 100

<sup>3</sup> Total does not include any figure in the 0–100 band



# Types of Requests

## 1. VOLUNTARY DISCLOSURES AT THE REQUEST OF A GOVERNMENT ORGANIZATION:

Refers to the voluntary disclosure of personal information at the request of law enforcement or other government organizations. These requests deal with circumstances where a warrant or court order is not required to obtain information, including but not limited to criminal investigations, information needed to locate and notify the next-of-kin of an injured, ill or deceased individual, return stolen property, or assist in the search for missing or lost persons.

## 2. VOLUNTARY DISCLOSURES ON THE INITIATIVE OF THE ORGANIZATION:

Refers to the voluntary disclosure of personal information to government authorities for the purpose of reporting a crime. In these circumstances, there is no request from government authorities.

## 3. DISCLOSURES IN EMERGENCY OR EXIGENT CIRCUMSTANCES:

Refers to requests made to assist law enforcement agencies in situations involving serious or imminent harm to any person or property without application to a judge. Requests made in emergency or exigent circumstances include but are not limited to requests for basic identifying information (referring to personal identifiers such as customer name, telephone number, mailing address and the local service provider identifier associated with a telecommunications or other service), intercepted communications, and tracking data (governed by relevant provisions of the *Criminal Code* including ss. 184.1, 184.4 and 487.11, and other relevant statutes and the common law).

## 4. DISCLOSURES MADE IN COMPLIANCE WITH FEDERAL OR PROVINCIAL LAW:

Refers to compellable requests made by government agencies under the express authority of federal or provincial legislation, such as the *Customs Act* or *Income Tax Act*, for regulatory enforcement or other government service purpose. These requests are sometimes referred to as "government requirement letters".

## 5. COURT ORDERED (WARRANTED) DISCLOSURES:

Refers to production orders, summons, subpoenas, and search warrants issued by a judge or other judicial officer. There are several different types of these orders, including but not limited to:

### a) Basic identifying information (court ordered):

Refers to personal identifiers such as customer name, telephone number, mailing address and the local service provider identifier associated with a telecommunications or other service provider in circumstances where there is a reasonable expectation of privacy, and disclosed pursuant to a court order.

b) Tracking data (obtained via tracking warrant; governed by s.492.1 of the *Criminal Code* and other relevant statutes):

Refers to data that relates to the location of a transaction, individual or thing.

c) Transmission data (obtained via transmission data recorder warrant; governed by s.492.2 of the *Criminal Code* and other relevant statutes):

Refers to any data obtained by dialing, addressing, routing, or signaling, such as the incoming and outgoing numbers of a phone call, or the time an email was sent and received. Transmission data does not reveal the content of a conversation or message.

d) Stored communications content and other stored data (obtained via warrant and production orders; governed by ss, 487, 487.01, and 487.014 – 487.018 of the *Criminal Code* and other relevant statutes):

May refer to the provision of historical data, including text message detail ( not content ), data such as photos, or the provision of other types of stored data.

e) Real time interception (obtained via wiretap warrant; governed by Part VI of the *Criminal Code* and other relevant statutes):

Refers to private communications intercepted by means of any electro-magnetic, acoustic, mechanical or other device.

## 6. OTHER:

a) Foreign agency requests (court ordered):

Refers to requests received from government agencies outside of Canada regarding criminal matters. The Government of Canada may facilitate such requests pursuant to the *Mutual Legal Assistance in Criminal Matters Act*.

b) Preservation demands and orders (governed by s.487.012 and s.487.013 of the *Criminal Code*):

Refers to demands (by peace or public officers) or orders (by a justice or judge) requiring a person to preserve computer data for either 21 or 90 days; depending on the circumstances. Preservation demands and orders simply compel a person to not delete data in their possession or control. This allows government agencies time to submit an appropriate request to obtain the preserved information, such as obtaining a court authorized production order to obtain historical text messages.





# Q & A

## WHY DOES SASKTEL DISCLOSE CUSTOMER INFORMATION?

Like all telecommunications companies that provide services, we are required by law to assist agencies for purposes such as enforcing criminal law, protecting public revenue and safeguarding national security.

We also aid emergency services agencies for reasons such as responding to life-threatening situations or dealing with matters relating to emergency calls. We only disclose customer information in accordance with the law, and we assess all requests for information to ensure they comply with the law.

## CAN I FIND OUT IF MY INFORMATION HAS BEEN DISCLOSED TO A GOVERNMENT AGENCY?

**Yes.** Where an access to information request has been made by our customer, SaskTel would seek the permission of the agency to disclose the information that has been released.

## DO YOU NOTIFY YOUR CUSTOMERS WHEN POLICE REQUEST THEIR PERSONAL INFORMATION?

**No.** SaskTel is not permitted under court orders to notify customers if a request for their personal information has been made by police. As a result, customers are not notified about lawful requests made by federal or provincial government agencies.

## DOES SASKTEL HAVE A DEDICATED GROUP FOR RESPONDING TO DATA REQUESTS FROM GOVERNMENT AGENTS?

**Yes.** SaskTel does have a dedicated group for responding to data requests from government agents and police. They are experts in the whole area of security, and are intimately familiar with investigative techniques.

## DOES SASKTEL RECEIVE MONEY OR OTHER FORMS OF COMPENSATION IN EXCHANGE FOR PROVIDING INFORMATION TO GOVERNMENT AGENCIES?

Some services are chargeable and permit SaskTel to recover the cost of performing the work to meet the request.



## DOES SASKTEL HAVE GEO-LOCATION INFORMATION THAT YOU MAY HAVE COLLECTED ABOUT ME, MY DEVICES, AND/OR ASSOCIATED WITH MY ACCOUNT?

**Yes.** SaskTel does not provide customers with geo-location services but does create such information to route calls over our wireless network, for example. This information would only be released to police under a court order or an emergency situation.

## DO YOU PROVIDE METADATA OR DIRECT ACCESS TO CUSTOMER DATABASES?

**No.** SaskTel does not provide metadata (without a court order) or direct access to our databases in any event. We only provide the information we are required to provide, and this information is retrieved directly by SaskTel employees.

## DOES SASKTEL RECEIVE REQUESTS FOR INFORMATION IN CIVIL CASES?

**Yes.** Release of information would be subject to a court order or with the written consent of the person whom the personal information concerns.

## HOW OFTEN DOES SASKTEL RECEIVE REQUESTS?

SaskTel does not control the volume of information requests. The volume is determined by the total number of active police investigations and investigations underway by federal or provincial government agencies that have legislative authority to request customer information from SaskTel.

## WHAT AGENCIES CAN REQUEST CUSTOMER INFORMATION FROM SASKTEL?

The following may not be an exhaustive list since many statutes may have investigative authority that we haven't dealt with:

RCMP, police within the meaning of the *Police Act*, Canadian Security Intelligence Service, Departments of: Environment, Highways, Liquor and Gaming, CN and CP Police, Canadian Parks, Chief Coroner, Ombudsman, Consumer Protection Branch, Saskatchewan Financial Services Commission, Canada Revenue Agency, Canada Border Services Agency and the *Enforcement of Maintenance Order Act*.





