A Guide to Transparency Reporting for Canadian Businesses Using the DIY Transparency Report Tool

Electronic version first published at www.telecomtransparency.org by the Telecom Transparency Project. The Telecom Transparency Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto.

This project was funded through the Canadian Internet Registration Authority's Community Investment Program. Through the Community Investment Program, CIRA funds projects that demonstrate the capacity to improve the Internet for all Canadians. The CIRA team manages Canada's country code top-level domain on behalf of all Canadians. A Member-driven organization, CIRA represents the interests of Canada's Internet community internationally.

Document Version 1.0.2

About Telecom Transparency Project and Open Effect

The **Telecom Transparency Project** investigates how telecommunications data is monitored, collected, and analyzed for commercial, state security, and intelligence purposes. The Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. The Citizen Lab focuses on advanced research and development at the intersection of information and communications technologies, human rights, and global security.

Core to the Telecom Transparency Project's work is interrogating the practices of telecommunications service providers (e.g. AT&T, Vodafone, and Bell Canada) that route data traffic between communicating parties and the mechanisms that third parties use to access the digital information that is endlessly flowing through telecommunications service providers' networks. Rendering telecommunications processes transparent will help citizens, politicians, and businesses understand how private or public, and how secure or vulnerable, their communications are to service provider-linked communications interferences and data disclosures.

Open Effect is a Canadian not-for-profit that conducts research and advocacy focused on ensuring people's personal data is treated securely and accountably. It uses a mix of policy and technical analysis methods to explore how digital services use personal data. Open Effect builds interactive advocacy tools to disseminate its work and empower individuals to learn about and exercise their rights online.

About the Authors

This document was written by Christopher Parsons and Andrew Hilts. The DIY Transparency Reporting Tool was developed by Andrew Hilts, of Open Effect.

Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Research Associate at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Andrew Hilts is the Executive Director and research lead at Open Effect, as well as a Project Associate of the Telecom Transparency Project. His research work and software development focuses on empowering citizens to exercise their digital rights online. He specializes in access to personal information. As a research fellow at the Citizen Lab at the University of Toronto's Munk School of Global Affairs, Andrew collaborates with researchers who are examining telecommunications industry transparency, web-based surveillance, and other forms of information controls.

About This Document

This document constitutes an initial release that is meant to help organizations understand the contours of developing and publishing holistic transparency reports. Such reports disclose how companies retain data, process requests for data that are made by government agencies, and report on the regularity at which companies have disclosed information to such authorities.

We will continue to develop this document and the software associated with it (DIY Transparency Report Tool), adding further details, expanded discussions, and guidance as more information becomes available to us. We welcome (and very much encourage) feedback, critiques, suggestions, and observations from other interested persons with expertise to contribute (whether practical, legal, scholarly, or technical). We are, in other words, seeking expert input concerning transparency reports, their production, and publication in Canada and further abroad.

Please send feedback to: christopher@christopher-parsons.com

Table of Contents

Executive Summary

Consumers and citizens are increasingly concerned about how the major organizations in their lives care for and protect their digital communications. On the one hand they want to know that such organizations are working to secure information from unauthorized parties such as disgruntled employees and external hackers. But they also want to know whether, and if so to what extent, government agencies can and do request access to their information. Such concerns about government access have remained pressing issues in Canada for over a decade and became even larger concerns following Edward Snowden's revelations of government agencies' mass intrusion into organizations' databases and, sometimes, organizations willingly colluding with the same intruding agencies.

Some organizations have become 'more transparent' in response to consumer and citizen anxieties. For many of the largest telecommunications-related companies in the world, this has led them to publicize how they receive and respond to government request for organizationally-held or –controlled information, as well as the regularity and rationales for their disclosures of information to government agencies. And companies that are both large and small receive such kinds of requests, though typically smaller organizations are challenged in proactively developing policies and public-facing documents that explain how they retain data, how they respond to lawful government requests for data, or the regularity at which such responses take place.

The DIY Transparency Report Tool is designed to help such smaller organizations develop holistic transparency reports. Such reports comprehensively explain to customers, citizens, and government agencies alike how an organization can, and does, receive and respond to government requests. It does so by guiding organizational members through the process of developing a holistic report, while empowering them to customize their reports to reflect their organizational profile. And, critically, the tool is entirely open source and operates where the organization decides, so sensitive information is never disclosed to another party until the organization makes that decision.

This document explains the rationales for developing the documents involved in holistic transparency reporting, as well as offering a guide so that organizations can generate their own holistic transparency reports. The section on **data retention guides** provides information that can help organizations think through how long they retain data which is either automatically collected, or voluntarily provided, by subscribers and users. In addition to detailing the legal reasons for why

organizations ought to possess this kind of data inventory, the section also outlines a possible categorization scheme to differentiate between the kinds of information that an organization might retain. The output is a short document that will serve as a data inventory of user- and subscriber-related information and be used for business planning, disaster management, and to ascertain what information is under the organization's control should government agencies request data from the organization.

The section discussing **government request handbooks** suggests how organizations can build public-facing guidelines to outline what processes government agencies ought to abide by when requesting information from the organization in question. The guidelines can help government agencies more efficiently request information from organizations in accordance with pre-determined organizational business processes. To help organizations develop these guidelines, this section discusses difference between voluntary and compelled disclosures of information, the types of disclosures that government agencies might make, as well as the rationales for making such documents available to government agencies and the public more broadly.

Some Canadian organizations have reported on how often they have received, and disclosed information in response to, government requests for information since 2014. Such reports, which we term **government requests reports**, help organizations' subscribers and users, as well as the general public, understand the regularity at which government agencies use their lawful powers to compel information which is under the stewardship of the report-issuing organization. The section includes definitions for each of the dominant criminal code powers used to compel information from organizations as well as a way organizations can count such requests in their own reports.

Each section that discusses one of the aspects of a holistic transparency report also includes a question and answer subsection. These subsections respond to concerns or questions that organizations might have while, also, anticipating potential questions that an organization's users or subscribers might have about the decisions made in generating the different kinds of reports.

Ultimately, organizations that develop and publish holistic transparency reports will help external parties understand how long data is retained and, as a result, realize the availability of organizationally-controlled data to third-parties. Disclosing these holistic reports will also help external parties understand the processes government agencies must adhere to in order to request access to such controlled

data, as well as the regularity and terms under which government agencies have sought access to such data. In isolation the components of a holistic transparency report make a statement of sorts; combined, they tell a story about the organization and its responsible stewardship of data entrusted to it by its users and subscribers.

Introduction

Transparency reporting has gained increased attention within telecommunications policy circles over the past six years, ever since Google began releasing such reports in 2010. Corporate and public interest in such reports accelerated following revelations that major Internet access and service providers were either providing information to the United States' National Security Agency (NSA) or having it accessed without the companies' knowledge, with sixty-one companies having released transparency reports as of February 2016. Such reports detail how often companies disclose information about their subscribers to government agencies and, in some cases, the laws that have compelled such disclosures as well as the processes that companies have developed to respond to government requests. More rarely they include, or indicate, how long companies retain information about their subscribers and customers.

Over the past several years a number of Canadian Internet companies, including Rogers, TELUS, Wind Mobile, SaskTel, TekSavvy, and MTS Allstream, have released transparency reports with varying regularity. Canadian companies' reports have included different gradients of data, to the effect of making it challenging to understand the extent of government surveillance. Moreover, the companies that have released transparency reports enjoy access to counsel and policy analysts to help develop such reports. Few small- or mid-sized companies enjoy similar resources, leaving them unable to readily develop or prepare their own transparency reports without incurring significant operational costs.

This document, and the accompanying DIY Transparency Reporting tool, are designed to alleviate some of the operational costs that small- and mid-sized businesses might otherwise incur in the process of developing their transparency reports. Each section of this document explains the core aspects that can go into developing baseline, holistic, transparency reports. The sections will assist organizations understand the components that make up transparency reports, the rationale for including all three aspects of such reports, and some of the data inventory categories associated with each aspect of a holistic report.

Section One provides an overview of transparency reporting. It describes the three aspects that go into creating a holistic report: data retention guides, government requests handbooks, and government request reports. Moreover, this section explains the value of such reports for businesses, consumers, and citizens. This section will prepare an organization to answer questions such as:

- “Why is transparency reporting important?”
- “Why might reporting benefit my business?”
- “What value does reporting bring to my consumers?”
- “What is the civic value of producing such reports?”

Section Two focuses on creating and publishing a report that summarizes an organization’s data retention periods. It notes the value of creating such a report for compliance under Canadian commercial privacy law, as well as how such reports can help organizations efficiently respond to court-ordered requests to produce data that may be held by the organization. The section then proceeds to outline a range of data types which may be retained by an organization to help them understand what might be included in their own guide, as well as provide answers to frequently asked question regarding data retention guides.

Section Three outlines the importance of, and helps organizations create, government request handbooks. Such handbooks can inform organizational policy around how to respond when an organization receives a lawful order for data from a government agency. It begins by discussing the importance of possessing such guidelines and addresses the likelihood of receiving a request before summarizing some of the kinds of requests that organizations may receive. It concludes by providing answers to a series of questions related to government requests handbooks.

Section Four helps organizations generate reports which detail how often government authorities have requested information or the assistance of the organization, both by way of court order and without such an order. The section begins by explaining the importance of such reports for industry members, an organization’s customers, and the public more generally. Subsequently it outlines some of the orders an organization may receive to preserve, produce, or otherwise operate its systems to facilitate lawful government surveillance orders. The section ends with a series of answers to frequently asked questions associated with government requests reports.

The **Conclusion** of this document reiterates the importance of generating holistic transparency reports and why they demonstrate an organization’s commitment to both responsible data stewardship and to assisting in lawful investigations meant to protect citizens.

Appendix I includes an installation guide for generating holistic transparency reports with the DIY Transparency Report tool.

Appendix II outlines how an organization can use the DIY Transparency Report tool to create holistic data retention guides.

Appendix III offers resources for organizations interested in generating a data retention guide, government requests handbook, or government requests report.

Section One: Overview to Transparency Reporting

Companies that provide telecommunications, domain registration, virtual private network, and apps on mobile devices all enjoy privileged roles in the lives of everyday Canadians. Canadians entrust these companies with some of their most sensitive information and use them to conduct intimate, though typically not illegal, activities: they look up medical information, register domains to host opinion websites, secure Internet activities from third-party snooping, and share contact information and other data stored on their mobile phones to play games, chat with friends, and otherwise enjoy the benefits of the digital economy. Companies routinely collect information pertaining to their users and subscribers in order to deliver services and products. And, sometimes, this information becomes of interest to government agencies such as law enforcement, tax authorities, and municipal governments.

Large companies, such as Google, Rogers, Microsoft, TELUS, and Facebook routinely produce what are called 'transparency reports'. The first transparency report was published by Google in 2010 to "start a conversation about censorship and surveillance"[1] and other companies have followed, especially after documents leaked by Edward Snowden revealed that many leading companies either complied with, or deliberately assisted, large-scale government surveillance. As of February 2016 there were sixty-one companies releasing reports that span industry categories such as Internet service companies (e.g. Yahoo!, AOL, Cloudflare, Dropbox), hardware/cloud companies (e.g. Microsoft, Apple), social media companies (e.g. LinkedIn, Pinterest, Facebook), and Internet access providers (e.g. Verizon, Rogers Communications, Vodafone).[2] Unlike these Internet giants, smaller companies with just a handful or few dozen employees are less likely to produce transparency reports because of the cost in researching how

The DIY Transparency Report tool is built to assist small- and mid-sized businesses more easily create transparency reports and thus keep pace with their often-larger competitors.

[1] MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle for Internet Freedom. New York: Basic Books.

[2] Micek, P. (2016, revised Feb 18). Transparency Reporting Index. Access. Retrieved March 15, 2016, https://www.accessnow.org/pages/transparency-reporting-index.

to create them, and then actually invest in their production and publication.

Relatively few companies knowingly brush up against national security or intelligence operations. But far more receive orders from federal, provincial, or municipal agencies, when officials are investigating criminal code violations, tax infractions, or other possible violations of Canadian or international law. The DIY Transparency Report tool is built to assist small- and mid-sized businesses more easily create transparency reports and thus keep pace with their often-larger competitors.

The rest of this guide for creating transparency reports is designed to help small- and medium-sized businesses understand what is involved in holistic transparency reports, help the businesses create each aspect of such transparency reports, and gives advice to common questions pertaining to releasing transparency reports.

The rest of this section:

- Describes the three 'links' that go into creating a holistic transparency report
- Explains the value of creating such reports for businesses, consumers, and citizens
- Answers questions about the importance, benefits, and broader values of publishing holistic transparency reports

A Holistic Transparency Report

Holistic transparency reports involve three components: an organizational data retention guideline, government requests handbooks, and government requests report. A **data retention guide** provides information about how long organizations retain information that is in their possession. Some kinds of information that organizations might retain include:

- Subscriber information (e.g. address, billing information, email address, etc.)
- Personally identifiable information (e.g. geolocation information, Internet protocol addresses, search history, etc.)
- Transmission data (e.g. web traffic logs, call logs, time/date of communications between users, etc.)
- Content data (e.g. messages sent/received by users, content posted to service, content transited by organization on behalf of users, etc.)

A data retention guide can help companies rapidly identify to third-parties, including users and government agencies, whether they possess information of interest to those parties. Moreover, evaluating the data under an organization's control can clarify whether data is being retained for a clear, and overtly stated, business purpose for an appropriate period of time. Principle 8 of Canada's federal commercial privacy legislation, the *Personal Information and Protection of Electronic Data Act* (PIPEDA), asserts that "personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information." Consequently, developing a data retention guide can dovetail with an organization's efforts to ensure it is complying with Canadian privacy law.

A government requests handbook details how an organization responds to requests from government agencies for information which may be controlled or accessible to the organization. Such handbooks help organizations professionally respond to such requests and assist government agencies format and communicate requests in a manner that will be quickly addressed by an organization. These handbooks might explain a little about an organization, whether the organization responds to voluntary (i.e. non-court ordered) disclosure requests, how requests from foreign government agencies are handled, whether costs might be sought for providing lawful assistance, and whether the organization will seek to notify its users of any requests. The handbooks will also clearly identify to whom, and how, government requests should be made and how the organization requires requesters to prove they are genuinely government agents.

Government requests reports summarize the number, and kind, of requests that an organization has received over the period of time covered by the holistic transparency report. Such reports list different kinds of request-types, such as voluntary types of requests, court-ordered types of requests, as well as foreign requests as well as preservation requests, along with how organizations responded to such requests. Responses might include fully, partially, or refusing/being unable to provide responses, and might also note the number of affected persons/accounts which were notified of the government agencies' request and possible subsequent disclosures.

Combined, these three components establish a **holistic transparency report**. Independently each of these components are useful for organizations and their stakeholders. In aggregate, however, they can help external parties understand

how long data is retained and, as a result, the availability of organizationally-controlled data to third-parties, assist external parties understand the processes entailed in government agencies requesting access to such controlled data, and finally the regularity and terms under which government agencies are seeking to access the data. In isolation the components of a holistic transparency report make a statement of sorts; combined, they tell a story about the organization and its treatment of data as it pertains to third-party attempts to access that data.

Value of Holistic Transparency Reports...

... for Businesses

Holistic transparency reports help organizations, first and foremost, have an understanding of their data inventory, processes in place to respond to government agencies' requests to access data those agencies think an organization possesses, and a way of publicizing the regularity at which such requests are made. By publishing all of this information customers, as well, can understand that an organization is only collecting information as required to provide professional services or goods and that any and all disclosures of data to government agencies follows from a defined and responsible process. This can enhance trust with consumers who might otherwise be hesitant to use an organization's services or purchase their products on privacy grounds.

... for Consumers

Customers benefit from holistic transparency reports by understanding, in plain language, how businesses collect and protect consumers' information. Privacy policies can be challenging to understand and particularly opaque when it comes to understanding how organizations respond to government agencies' lawful requests for consumers' information. By consulting a holistic transparency report consumers can be assured that only information that is needed to provide a service or product are being collected and that businesses require government agencies to meet certain criteria before any data is released. Finally, consumers can evaluate whether government agencies are adequately scoping their requests by consulting the regularity at which government agencies actually request, and receive, data controlled by the organization.

... for Citizens

While governments of Canada are statutorily obligated to produce interception reports, which document how often agencies receive warrants to conduct live telecommunications, video, and auditory surveillance, they are not similarly required to report on all the other kinds warrants and data production orders they

can lawfully obtain. The result is that government agencies are highly unlikely to disclose how often they use their powers barring significant legislative reforms. Consequently, citizens who wants to understand how, how often, and how appropriately government agencies use the powers they possess must rely on businesses and organizations to publish transparency reports. Without such reports citizens cannot understand the scope, and scale, at which government agencies request, or gain access to, citizens' data and thus cannot engage in empirically-grounded discussions about the (in)appropriateness of such requests.

Broader Value of Holistic Transparency Reports

Organizations are not required by law to develop or produce transparency reports. But producing transparency reports constitutes a form of corporate social responsibility: the reports both demonstrate responsibility in handling the information that the organization is entrusted with, responsibility in honoring privacy assurances companies provide to their customers, and responsibility to the broader community in which the organization is situated. In effect, holistic reports functionally improve the well-being of all stakeholders which possess an interest in an organization that manages the information under its control.

Holistic transparency reports are not designed to shame or ostracise companies that respond to lawful requests but to strip away the fear, uncertainty, and doubt pertaining to how and how often lawful requests are issued by government agencies. Only by raising awareness of how such powers are used can organizations, parliamentarians, and citizens – to say nothing of government agencies themselves! – understand whether additional safeguards or limitations or restrictions are genuinely needed, or whether existing processes embedded in the law and organizational policies are sufficient to defray improper or excessive government activities.

… producing transparency reports constitutes a form of corporate social responsibility: the reports both demonstrate responsibility in handling the information that the organization is entrusted with, responsibility in honoring privacy assurances companies want to demonstrate to their customers, and responsibility to the broader community in which the organization is situated.

So, while high-minded, the broader value of holistic transparency report is to improve the basic states of knowledge that are needed to understand, and adjust as needed, the contours of government authority to intrude upon organizations' and citizens' freedoms. Fortunately, achieving these values requires relatively little day-to-day effort, and instead entails just collecting information that pertains to existing legal obligations (i.e. recording how often data is retained to ensure it accords with Canadian federal commercial privacy legislation), accounting for the conditions under which organizations disclose or share information with government agencies, and tabulating the regularity at which such disclosures are requested or take place.

Section Two: Data Retention Guide

Canadian commercial organizations collect information about their users and subscribers in the course of providing routine business services. This kind of information can be collected automatically – such as when a prospective or current customer either accesses a service and the organization logs that access – or by manual collection – such as when a user or subscriber communicates with the organization, provides payment information, signs up for an organizational account, or inputs information to receive a product.

Organizations may choose to retain collected or processed data for different periods of time based on the kinds of services/products they offer, their business models or plans, or government regulations associated with subscriber or other information. Many organizations will denote these kinds of rationales for retaining information in either their terms of service or privacy policy policies, but the statements in such organizational documents tend to leave unstated what data is specifically retained and for how long.

A **data retention guide** provides information about how long an organization retains information that is in its possession. Some kinds of information that organizations might retain include:

- Subscriber information (e.g. address, billing information, email address, etc.)
- Personally identifiable information (e.g. geolocation information, Internet protocol addresses, search history, etc.)
- Transmission data (e.g. web traffic logs, call logs, time/date of communications between users, etc.)
- Content data (e.g. messages sent/received by users, content posted to service, content transited by organization on behalf of users, etc.)

The Value of a Data Retention Guide

Data retention guides can help companies rapidly identify to third-parties, including users and government agencies, whether they possess information of interest to those parties. Moreover, evaluating the data under an organization's control can clarify whether data is being retained for a clear, and overtly stated,

business purpose and whether data is being retained for the appropriate period of time. Principle 8 of Canada's federal commercial privacy legislation, the *Personal Information and Protection of Electronic Data Act* (PIPEDA), asserts that "personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information." Consequently, developing a data retention guide can dovetail with an organization's efforts to ensure it is complying with Canadian privacy law.

… developing a data retention guide can dovetail with an organization's efforts to ensure it is complying with Canadian privacy law.

Elements of Data Retention Guidelines

Organizations may already possess unofficial, internal, data retention guidelines that record how long business-pertinent data produced by users or subscribers is retained. Moreover, consulting existing log files may reveal how long automatically collected information – such as that collected by networking appliances or by crash logs or other automated software reporting processes – is retained in organizational databases. The following parts of this section outline how different categories are understood/defined in the DIY Transparency Report tool, as well as what is involved in generating each section of an organization's Data Retention Guide using the DIY Transparency Reporting Tool.

Personal Access Rights and Canadian Law

Canadian privacy law empowers Canadian residents to serve legally binding requests on companies, which compel companies to disclose the information they collect or retain about the residents. Responses must be provided within just a few weeks. Having a data retention guideline can facilitate responding to consumers by ensuring that companies know what data is collected and where it is likely located in organizational systems.

Categories of Data Retained by Organization

The DIY Transparency Reporting Tool lets organizations explicitly assert what information they retain and for how long. The following identifies the most common kinds of data that organizations might retain. To generate a Data

Retention Guide an administrator will select the 'classes' of data that are retained (e.g. **subscriber data**, **personally identifiable information**) and the associated 'types' of information retained for each of those classes (e.g. address, email, billing information, geolocation). Organizations can also generate a narrative, or descriptive body of text, to contextualize their data collection activities.

Subscriber Data

Organizations routinely collect **subscriber information** in the course of providing services and fulfilling product orders. It lacks a formal legal definition, but subscriber data generally includes the following types of information/identifiers:

- Address
- Billing information
- Email address
- Phone number
- User name assigned/chosen by subscriber

Depending on the organization in question, it may collect additional information such as:

- Account numbers
- Account creation/last sign in dates
- Shipping or payment locations
- Registered mobile phone number
- Other information associated with the subscriber's profile that are either generated by the organization or that the subscriber provides as part of joining/using the organization's service

Personally Identifiable Information

Even if an organization is not using information in its possession to identify individual users, the collected information may still constitute **personally identifiable information**. Section 2(1) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) states that "personal information" means "information about an identifiable individual." Canadian court decisions mean that this definition should be given a broad and expansive interpretation. In part, this means that:

- Information "about" an individual can merely relate to an individual
- Information can be personal while simultaneously pertaining to more than just one person

- Even public information can be personal, and that what is often core to the definition is that an individual is *identifiable* by way of the information, even if they are not *identified* using it[3]

Some types of information collected by organizations, and which often is classified as personally identifiable information, includes:

- Geolocation information
- Internet protocol addresses
- Websites visited (on an organization's own webpage)
- Websites visited (using a service provided by the organization)
- Search histories retained by the organization
- Call logs

This is a non-exhaustive list, however, and organizations should consider the information they automatically collect, or which is provided by subscribers, that in the hands of the organization could be used to identify individuals who use the organization's services or products.

Content Information

Some organization transit or store communications (e.g. Internet browsing, email, chat-based communications) or documents (e.g. as a file locker service, a hosting service) or otherwise can access the words, images, sounds, or other content-defining characteristics of communications. In some cases, **content information** will be retained by an organization in order to provide services or to comply with internal business processes (e.g. retaining communications between a user and the organization for future dispute resolution purposes).

Organizations may need to customize the kinds of data which are reported in their data retention guide to accommodate their organizations' business processes and practices. Options that are provided by default by the DIY Transparency Report tool are deliberately generic and, as such, may not fully account for the content stored by organizations.

Transmission Data

Transmission data refers to information associated with dialling, addressing, routing, or signalling, such as incoming and outgoing times of calls, non-content information

[3] For more, see: Office of the Privacy Commissioner of Canada. (2015, revised Dec 11). Legal information related to PIPEDA: Interpretation Bulletin. Retrieved June 1, 2016, https://www.priv.gc.ca/leg_c/interpretations_02_e.asp.

associated with text messages or chat-based communications, or other data that does not reveal the content of the communication or message. Transmission data is more commonly known as 'metadata'.

Additional kinds of metadata might be times that a subscriber accesses websites, but without the full URLs of the websites accessed, or other kinds of information that are associated with communications but not constitute communications themselves. It is possible that an organization might retain transmissions data associated with content, but not the content itself: as an example, an organization might retain call logs but not recordings of the calls themselves.

Organizations may need to customize the transmission data items in the DIY Transparency Report tool to reflect their practices and services offered.

Other Types of Data

Clarifying Narrative or Description

In addition to the aforementioned types of data, an organization might want to provide non-structured information to readers. Such information might include information on why it specifically retains the information it does, the security or other controls that have been established to delimit access to the information, or explanations of why different business systems require the data outlined in the organizational data retention guideline to provide services to individuals.

Organizations may also include contact information with their data retention guide, so that customers and subscribers can contact the organization to provide feedback on how, why, and how long data is retained.

Furthermore, this non-structured information might include licensing information (is the document copyrighted, protected under a Creative Commons license, etc.) as well as a FAQ that provides answers to common questions that readers of the data retention guideline might regularly ask the organization.

Generating a Data Retention Guide using the DIY Transparency Report Tool

See **Appendix II** for instructions on creating a data retention guide.

Possible Questions About Data Retention Guides

Q: I have one hundred things to do. Why should I prioritize writing aa data retention guide?

A: Federal commercial privacy law asserts that organizations shouldn't collect, or

retain, information that isn't pertinent to their business operations. But organizations can derive benefits beyond complying by developing and publishing a data retention guide. To begin, such a guide can clarify whether business systems are collecting data in excess of what is stated in privacy policies, as well as force organizations to identify and evaluate the various kinds of data that are under their control; doing so, an organization might realize there are further business opportunities that are latent in the data they collect or, in contrast, cost efficiencies associated with collecting less data.

Q: What is the cost of not producing one of these guides?

A: The cost varies depending on the size and complexity of the organization's operations. But understanding data that is collected or otherwise under the control of an organization can clarify whether it is incurring costs for data storage in excess of business needs, as well as whether collected data is adequately noted in the organization's privacy policy. Moreover, by producing one of these guides an organization will be well suited to identifying the kinds of information that might be affected in the case of a data breach, instead of having to perform both a data inventory and breach analysis simultaneously.

Q: How long will it take to develop these guides?

A: The time to develop an organization's data retention guides vary depending on existing documentation, organizational size, and service complexity. In effect, the time to create the guide using the DIY Transparency Report tool itself is minimal, whereas the time to collect data to input information into the DIY Transparency Report tool varies on a per-organization basis.

Q: What's the difference between subscriber information and personally identifiable information? Or between content or transmission information and personally identifiable information?

A: Subscriber information is, by default, personally identifiable information. In contrast, not all personally identifiable information is classified as subscriber information. Moreover, government agencies sometimes specifically request subscriber information and differentiate such requests from broader or more general production orders that pertain to information pertaining to a specific user or subscriber. So personally identifiable information is that which is separate from, or distinct from, the personal information that is associated with a subscriber's profile that is accessible to the organization.

Similarly, transmission data or content data can often identify a person and, thus, constitute personally identifiable information. However, content and transmission data is not always personally identifiable, though may be linked to an identified person. As a result, personally identifiable information functions as a separate, and more specific, set of data elements from other categories of data that do not always contain just personally identifiable information.

Q: Won't disclosing how long I retain data scare away subscribers or users?

A: Organizations routinely collect and retain data in order to provide services or deliver products to subscribers or users. Explaining why certain data is retained in the narrative section of the data retention guide can help an organization manage users' expectations and assuage concerns, thus mitigating any detrimental impact(s) of publishing these kinds of guides.

Q: Who really cares about this information?

A: Principally, it's members of your organization that most likely care the most about these guides. Beyond ensuring that its operations are within the scope of Canadian law, knowing what data is being collected may reveal business opportunities, areas where efficiencies can be realized by collecting less data, or even where additional data might be useful for improving service delivery. Moreover, should a government agency request information from your organization you will likely know whether you actually retain the requested data and, if so, are more likely to know where it's kept and for what period of time you retain the type of data of interest to the agency.

Q: Why does developing my organization's data retention guide matter from a cybersecurity standpoint?

A: Organizations suffer intrusions and data breaches on a regular basis. Should your organization suffer an intrusion or breach, knowing what data you retain and for how long, and even in which systems, may help to ascertain the number of subscribers or users who have been affected.

Parliament has passed data breach legislation though the breach notification requirements have not come into force as of June 2016. However, organizations will be obligated to disclose when a breach occurs and its severity once that legislation is in force. An organizational data retention guideline may accelerate such analysis and reduce the costs of dealing with a future intrusion or breach.

Q: How should I publish my organization's data retention guide?

You may choose to include your data retention guide as a link in your privacy policy, within your company's corporate social responsibility documents or strategy, or other public-facing sections of your organization's website where you post privacy-related information.

Q: Where are resources to learn more about data retention, and data retention guides?

Appendix III of this document includes resources concerning data retention and data retention guides.

Section Three – Government Requests Handbook

Organizations which process, or store, data on behalf of their users or subscribers may sometimes receive requests from government agencies seeking to access information under an organization's control. Larger organizations, or those with on-staff counsel, may have internal capacity to evaluate, process, and respond to such requests but the same is less common for small- and medium-sized organizations. For these smaller organizations it can be helpful to establish how, and in what ways, such requests will be responded to ahead of receiving an actual request in order to both streamline and facilitate responses to government agencies, and to assist both government agencies as well as the organization's users or subscribers to understand how it will, and will not, respond to government agencies' requests.

There are a variety of types of requests that an organization might receive and different kinds of disclosures. Some organizations might require a court order or other kind of compulsory demand before disclosing information, whereas others may respond to informal or non-compulsory requests for information. Others might voluntarily share information with some government agencies if they detect unlawful or suspicious behaviour on the part of their users or subscribers, or as a result of their service being used in questionable manners. An organization's privacy policies will often include provisions stating that information may, under some circumstances, be disclosed or shared with government agencies: government request handbooks clarify for all involved what, specifically, such provisions actually mean in practice.

An organization's privacy policies will often include provisions stating information may, under some circumstances, be disclosed or shared with government agencies: government request guidelines clarity for all involved what, specifically, such provisions actually mean in practice.

A **government requests handbook** explains how an organization receives, processes, and discloses information pertaining to government agencies' requests for information under the organization's control. Some of the elements of a government request handbook include:

- When the document was created

- What identifying information requesting government agents must include with requests
- Whether an organization will voluntarily share information, or if it only responds to court ordered, statutorily compelled, or emergency/exigent requests
- Clarification about whether the organization commits to notify affected parties of the requests
- Information pursuant to cost reimbursement for responding to government requests

The Value of Government Requests Handbooks

When government agencies contact organizations for information, they sometimes possess incomplete or incorrect information concerning what information an organization controls. Moreover, government requests for information are sometimes informal or issued by foreign government agencies that may be unable to legally compel the company to disclose information. Developing a government request handbook serves multiple purposes.

First, developing a handbook encourages an organization to consider what information it possesses and the terms under which such information will, or will not, be disclosed to government agencies. Establishing and publishing a government requests handbook before receiving a request from a government agency means that an organization's responses are thoughtful as opposed to being created ad hoc, and established in a way to ensure lawful compliance while simultaneously maintaining the trust of its users or subscribers. Second, published government requests handbooks help government agencies understand the process an organization has established and ensure that any agency's requests meet the legitimate requirements established by

Establishing and publishing a government requests handbook before receiving a request from a government agency means that an organization's responses are thoughtful as opposed to being created ad hoc, and established in a way to ensure lawful compliance while simultaneously maintaining the trust of their users or subscribers.

How Likely Is It That A Government Agency Will Request Our Data?

Government agencies are increasingly attentive to the information that are retained by organizations large and small. Small development studios which create applications for mobile devices, organizations that develop virtual private networking software, and organizations that provide website or content hosting, as well as communications services, could receive a request from a government agency. The likelihood of receiving a request is challenging to divine because government agencies are not required to publish how often they use the majority of their powers. So a government request guideline document functions as a kind of preparatory insurance: it ensures an organization has considered how it will respond to such requests while also indicating to government agencies that they will have to adhere to a functional process and, perhaps, be less likely to try and simply pressure information from organizations.

the organization; this can accelerate the pace at which lawful requests are responded to by the organization, instead of the organization and requesting agency exchanging multiple communications before the organization actually starts responding to the request itself. Third, by publicizing its government requests handbook an organization can showcase to its users and subscribers that it is a responsible steward of the information they entrust to the organization in question and, moreover, means that individuals can provide direct comment on an organization's actual practices.

Elements of a Government Requests Handbook

Government request handbooks provide sufficient information that government agencies can clarify what kinds of requests a company is willing to receive, and the preferred ways for government agencies to serve such requests on the organization. These handbooks can also, as part of a narrative, explain the kinds of information that are/are not available. These kinds of explanations can be facilitated by organizations also issuing a **data retention guide** so that government agencies do not spend time requesting access to information that the organization does not, or no longer, retains.

Handbook Categories

Date Updated

Government agencies and interested users or subscribers, as well as citizens, need to know that they are reading an organization's current government request handbook. Readers need to know what an organization's current policies are; excluding this information could cause an organization to receive requests from government

agencies that are accidentally using out-of-date versions of the organization's handbook.

What is Our Service

Government agencies may not entirely understand the nature or type of service that is provided by an organization. By including a narrative discussion of their services, organizations might explain what kinds of services or products they offer, as well as clarify the kinds of information that are explicitly not collected as part of the service or product offerings. These narrative discussions might be very brief for small application developers, or longer for organizations offering a range of services such as virtual private networks, or organizations that provide hosting, email, and domain registration services.

How to Serve a Request

Organizations may prefer to receive requests from government agencies at a certain fax number, phone number, email address, or web form in order to facilitate faster responses. Ideally, government agencies will have a specific way of communicating with the organizations and, also, know either the specific person to communicate with or the relevant title of the person in the organization (e.g. President, Owner, Legal Department, etc.).

Required Contact Information

Organizations may request that government officials making requests provide information that is used to ensure an actual official for a government agency, as opposed to a person masquerading as an official, is making a request. To authenticate an official, an organization might require that requests identify which agency is making the request, the official's badge number or employee ID, the requestor's official email address, the official's phone number with extension, or the official mailing address for the agent in question.

Organizations may also request that government agencies state the time by which they require a response. This information can help both the organization and agencies better understand the time-sensitivity of the request being made.

Types of Organizational Disclosures

Though organizations are required to comply with lawful requests, such as government statutory requests (sometimes referred to as 'government requirement letters'), court orders, or exigent circumstances requests, they can adopt different policies concerning how they respond to informal or non-compulsory requests for information as well as how they respond to requests from foreign government

agencies. Moreover, organizations may note the conditions under which they will initiate voluntary disclosures of information to government agencies.

Non-Obligatory Requests for Information
Government agencies will sometimes contact organizations to request that information be disclosed without first obtaining a court order and without conditions which would enable the agencies to otherwise compel the organization to disclose information. Organizations should indicate whether they are receptive to receiving such requests and subsequently disclosing information and, if so, whether such disclosures will pertain to specific kinds of requests (e.g. serious crimes, tax fraud, child abuse).

Policy on Exigent Requests
Government agencies sometimes request organizations to either disclose information or provide assistance in exigent, or emergency, situations (e.g. to prevent or stop an imminent serious crime, respond to a distress call from a victim) where the agency in question does not have the time to first obtain a court order. Organizations might have unique contact information for processing such requests, include information about how quickly they can respond in exigent circumstances, or otherwise identify policies they have developed to respond to such pressing types of requests.

Responding to International Requests
Organizations may receive requests from non-Canadian government agencies to provide the agencies with information accessible to, or under the control of, the organization in question. Canadian law does not bar Canadian organizations from providing information to foreign agencies, though organizations may decide to require foreign agencies to serve requests vis-à-vis the *Mutual Legal Assistance in Criminal Matters Act*. Per this Act, Canadian agencies are granted legal authority to obtain court orders on behalf of countries that are part of mutual legal assistance treaties with the Canadian government. In effect, if organizations require foreign orders to be channeled through Canadian agencies it ensures that any requests, and subsequent disclosures, comply with Canadian legal standards.

User Notification
In the event that government agencies request information pertaining to an organization's users or customers, the organization may commit to notifying those who are affected by the requests. Government agencies are generally not required to notify individuals of requests unless it involves a live interception of communications data or the disclosed information is entered into evidence against the persons affected. Consequently, unless an organization notifies the affected persons they are

unlikely to ever know a government agency possessed an interest in information pertaining to them. In some, though not all cases, a court order may bar the organization from notifying those affected; thus organizations may prefer to assert that they will notify those affected when it is lawful to do so.

Cost Reimbursement
Fulfilling government agencies' requests may generate financial costs for the organization that either possesses, or controls, the information being sought. Organizations may state they will seek reimbursement where appropriate or assert they will not seek reimbursement for assistance provided to government agencies.

Narrative
Organizations may want to explain to both government agencies and its customers or users alike the rationales driving some of its decisions concerning how government requests are received and processed, and explain what kinds of data are available or unavailable given the organization's practices. Moreover, additional information concerning what an organization will do when overwhelmed with requests might be appropriate, and the organization might even go so far as to direct government agencies towards online or paper forms that they prefer be included when agencies submit requests.

Organizations may also include contact information with their government requests handbook, so that customers and subscribers can contact the organization to provide feedback on the company's policy concerning its policies associated with government requests.

Furthermore, this non-structured information might include licensing information (is the document copyrighted, protected under a Creative Commons license, etc.) as well as a FAQ that provides answers to common questions that readers of government requests handbook might regularly ask the organization.

Generating a Government Requests Handbook Using the DIY Transparency Report Tool

See **Appendix II** for how to create a government requests handbook.

Possible Questions About Government Requests Handbooks

Q: Will I get more requests from government agencies if I publish one of these handbooks?

A: There is no reason why publishing a government requests handbook will result in additional requests from government agencies. In fact, by clarifying the conditions under which your organization will, or will not, disclose information you may see fewer requests (e.g. you may receive fewer requests for information absent court orders or statutory authorities, if your organization requires court orders or statutory authority before providing data in response to any request.)

Q: How long will it take to develop my organization's government request handbook?

A: It shouldn't take too long to actually generate a draft handbook using DIY Transparency Report tool; the output of the tool can be adjusted as desired, and then published online or retained internally for when/if a government request is received. However, actually determining the kinds of policies that your organization adopts can take more time and we cannot provide guidance on how long your specific organization will take to craft such policies.

Q: Shouldn't I just always give government agencies what they ask for?

A: Your organization may adopt a policy of always disclosing information to authorities in all cases. The government requests handbook serves to help government agencies, and if published publicly your organization's subscribers or users, to understand how you treat requests.

Q: What do I do when I think a court order is overbroad?

A: If you believe that a government authority is requesting more data than is appropriate you should contact competent counsel.

Q: Why wouldn't I always respond to a court order, regardless of the jurisdiction issuing it?

A: Your organization may develop a policy of always responding to court orders. Canadian law currently authorizes such decisions. However, organizations may want to internally establish – and publicly explain – whether and how they evaluate foreign court orders. Does your organization ensure that the issuing country meets company-researched rule of law standards? Does your organization ensure that the orders are not designed to, and will not, control or stifle legitimate speech? Does your organization only respond to foreign requests when the requesting government or country meets certain human rights standards?

Q: What's the problem with just making up my requests handbook as needed?

A: Many organizations develop policies for responding to government requests at the

time that they are first contacted by authorities. A challenge – based on our discussions with small- and medium-sized organizations – is that establishing the correct precedent for an organization can be challenging when a government official is aggressively asserting their need to access data. Having a handbook in place helps to facilitate a calmer and better managed discussion with a requesting agency official and the representative of the organization.

Q: What's the cost of not producing one of these handbooks?

A: Government requests handbooks are designed to streamline, and make more efficient, an organization's engagements with government agencies. Not developing such a handbook can result in an organization having to pivot from a pressing business issue to craft handbook responses. In effect, by preparing for government request it's less likely that your organization will experience a significant disruption due to figuring out how to respond to requests, should a request be received.

Q: How do I know what information is, or isn't, available to government agencies?

A: Government agencies might request information that your organization doesn't possess, or doesn't believe that it controls. In order to promptly respond to requests organizations can develop a data retention guide, as discussed in Section Two. Such data retention guides will ensure your organization knows what information is available and whether the data requested is even in the control of your organization.

Q: How much money can I charge for helping government agencies access data about my customers or users?

A: The amounts of money you can request for assisting government agencies varies based on which type of agency (e.g. domestic or foreign) is making the request and sometimes based on the powers (and accompanying authorizing legislation) being invoked. Competent counsel can help your organization develop specific fee schedules if they are needed.

Q: Who really cares about this kind of information?

A: Government agencies making requests will likely care; your government requests handbook can include whether you'll respond to requests to voluntarily disclose information, the person(s) to whom requests should be sent, and perhaps even the kinds of information which are available if you link your government requests handbook with your organization's data retention guide. In effect, a government request handbook can ensure that government agencies can more efficiently engage

with your organization.

Your subscribers and customers may also care, insofar as your handbook will clarify how you secure and steward their information. Privacy is increasingly a topic of concern and publishing your handbook may help assuage any concerns that your subscribers or customers have about your organization's management of their information.

Q: What does the government think of me issuing a government request handbook?

The Office of the Privacy Commissioner of Canada, along with other international privacy and data protection commissioners, supports organizations releasing both government request reports and government requests handbooks.[4]

Q: How should I publish my organization's government requests handbook?

You may choose to include your government requests handbook as a link in your privacy policy, within your company's corporate social responsibility documents or strategy, or other public-facing sections of your organization's website where you post privacy-related information.

Q: Where are resources to learn more about government requests handbooks?

Appendix III of this document includes resources concerning government requests handbooks.

[4] See: "Resolution on Transparency Reporting," *The 37th International Conference of Data Protection and Privacy Commissioners*, Amsterdam, October 27, 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/15-10-27_Resolution_Transparency_Reporting_EN.pdf.

Section Four: Government Requests Reports

Canadian organizations routinely collect or process information on behalf of their users/subscribers in the course of providing business services. This information can be helpful to investigate, or solve, investigations conducted by government agencies for criminal, tax, import, or other purposes. Due to the potential value of this information in assisting government activities, government agencies sometimes request or compel organizations to disclose certain information.

Companies may voluntarily provide information to government agencies when informal requests are made – such as a government official calling or emailing a company to ask for information without first receiving and serving a court-backed order on an organization – or following the receipt of a warrant or other court order. Moreover, organizations can choose to comply fully with a request or order, or can choose to challenge orders they believe are inappropriate, such as because the orders are overly broad in nature. Moreover, organizations might share information with government agencies of their own volition when they believe that doing so is needed to proactively stop a criminal activity, or when they suspect that a user or subscriber is acting unlawfully.

Government requests reports document the regularity at which organizations receive, and how they respond to, government agencies' requests for information. They are often referred to as 'transparency reports' by industry groups and members of civil society. Broadly, government requests reports account for how often information is:

- Voluntary provided to government agencies
- Mandatorily provided under government statutes
- Compelled to be provided pursuant to a court order
- Disclosed to foreign governments' agencies
- Preserved or retained, to be disclosed only following the requesting government agency serves a production order on the organization

The Value of a Government Requests Report

Organizations develop and issue government requests reports to showcase the

regularity at which they do, or do not, disclose information to government agencies. These reports demonstrate that an organization is committed to providing data when lawfully required to do so and, in requiring such, operates as a careful steward of its users' or subscribers' information. Canadian Internet companies began releasing government requests reports in 2014. Rogers Communications and TekSavvy Solutions were the first Canadian companies to release such reports, and have since been followed by TELUS, SaskTel, Wind Mobile, and MTS Allstream.

These reports demonstrate that an organization is committed to providing data when lawfully required to do so and, in requiring such, operates as a careful steward of its users' or subscribers' information.

Government requests reports also support a broader social purpose of showcasing to subscribers, to industry colleagues, and to citizens more broadly how often government agencies are using their lawful powers to compel information from organizations. While government agencies have received additional powers in recent decades to combat criminal offenses, they have not been statutorily required to publicly report on how often they use those powers. Some Canadian companies have issued government requests reports in order to both showcase their stewardship of users' or subscribers' data, as well as to "encourage the Government of Canada to issue its own report[s]"[5] concerning government agencies' requests to organizations for information they either retain or process.

Elements of a Government Requests Report

Depending on the volume of requests received by organizations the organization in question may internally know of how often they are receiving, and responding to, government agencies' requests for information or assistance. However, even if this information is tracked internally an organization's users or subscribers are likely unaware of the regularity at which such activities take place. A government requests report conveys this information to parties external to the organization and, for organizations that lack an internal method of tracking these requests, provides a method for organizations themselves to record the regularity, and kinds, of requests made by government agencies. The rest of this section proceeds by defining various kinds of government agencies' orders that are associated with the *Criminal Code* and

[5] Rogers Communications. (2014). Rogers Communications 2013 Transparency Report. Rogers. Retrieved December 14, 2014, http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf.

then responds to frequently asked questions about government requests reports.

Reporting Categories

Voluntary Disclosure Following Government Request

Government agencies will sometimes ask organizations to voluntarily provide certain information to the requesting authority. In some cases these requests may be made where the agency does not believe a warrant or court order is required to obtain the information, such as when conducting criminal investigations, to location or notify next-of-kin, return property, or help search for missing persons. Organizations are permitted to ask the requesting agency to return with a court order or explain what statute requires the disclosure before volunteering the requested information.

Voluntary Disclosure at Organization's Initiative

Organizations may voluntarily share information with government agencies, though organizations may prefer to consult with counsel before doing so in order to ensure they are properly respecting any terms of service, contracts, or other guarantees made between the organization and its customers/subscribers/users, as well as acting in compliance with Canadian law. When voluntarily disclosing information the organization provides information without the receiving government agency in question first requesting the relevant information.

Disclosure in Emergency or Exigent Circumstances

Government agencies may sometimes request rapid or immediate access to information retained by organizations due to exigent circumstances, where the agencies would normally require a court order to access the information in question. Such requests may be for: identifying information (e.g. customer name, telephone number, mailing address, email address, or other information needed by the organization to identify its subscribers or customers) as well as communications content or transmission data.

Disclosures to Comply with Federal Law

Federal government agencies may sometimes compel organizations to disclose information by exercising statutory authorities; this means that the agencies do not require a court order to compel the information from an organization. Some organizations refer to these as 'government requirement letters'.

Disclosures to Comply with Provincial Law

Provincial government agencies may sometimes compel organizations to disclose information by exercising statutory authorities; this means that the agencies do not require a court order to compel the information from an organization. Some

organizations refer to these as 'government requirement letters'.

Court Ordered (Warranted) Disclosures:

Court ordered disclosures refer to production orders, summons, subpoenas, and search warrants that are issued by a judge or judicial officer. They compel a company to collect and disclose information under the organization's control. In some cases an organization may challenge the disclosure of the information prior to disclosing it to the requesting government agency. Organizations should consult with counsel to determine their legal options in responding to court ordered disclosures of information to government agencies.

There are many different types of court ordered (warranted) disclosures. Some of the most common types of disclosures are included in the DIY Transparency Reporting Tool by default, and include:

Basic identifying information (court ordered)

Such orders compel an organization to collect and disclose personal identifers associated with a subscribers/customer/user. Identifiers may include customer name, telephone number, mailing address, email address, or other identifiers needed to identify a person where those identifiers enjoy a reasonable expectation of privacy and can only be disclosed pursuant to a court order.

Tracking data

Tracking data orders are obtained using *tracking warrants*, as denoted under s.492.1 of the *Criminal Code*. These orders are used to obtain data that relates to the location of a transaction, individual, or thing.

Transmission data

Transmission data orders are obtained using a *transmission data recorder order*, as denoted under s.492.2 of the *Criminal Code*. These orders are used to obtain data that is obtained by dialling, addressing, routing, or signalling, such as incoming and outgoing times of calls, non-content information associated with text messages or chat-based communications, or other data that does not reveal the content of the communication or message. Transmission data is more commonly known as 'metadata'.

Stored communications and other stored data

Stored communications and other stored data is often obtained using a *warrant* and *production orders*, as denoted under s.487, 487.01, and 487.014-487.018 of the *Criminal Code*. These orders may refer to historical data that includes the content of stored communications including email, chat messages, photos, documents, or any other

kinds of stored data.

Real time interceptions
Real time interceptions are often obtained using a *wiretap warrant*, as denoted under Part VI of the *Criminal Code*. These orders may refer to private communications which are intercepted by means of electro-magnetic, acoustic, mechanical, or other means and involve the live capture of communications that are intermediated or accessible by the organization.

Foreign Agency Requests (Court Ordered)

Canadian organizations may sometimes receive requests from non-Canadian agencies for access to information held by to Canadian organization. Such orders may be accompanied by a court order from the agency's jurisdiction. Alternately, the foreign order might be facilitated by Canadian agencies per the *Mutual Legal Assistance in Criminal Matters Act*.

Preservation Demands and Orders

Preservation demands and orders can be obtained under s.487.012 and 487.013 of the *Criminal Code*. Demands are made by peace or public officers whereas orders are made pursuant to judicial authority. These orders compel an organization to retain to identified information for 21 days (for domestic demands and orders) or 90 days (where the demand or order is made in order to assist an international investigation). Organizations are not required to disclose information prior to receiving a production order from the agency which served the demand or order.

Production orders are used to compel information from organizations, often after the organization has previously been compelled to preserve information after receiving a preservation demand or order. The preservation demands and orders category is used to identify the frequency at which preservation demands or orders are received, whereas the disclosure of actual data is reflected in one of the relevant court ordered disclosure categories.

Tabulating Reporting Categories

Each reporting category there a series of qualifying fields that contextualize requests.

Number of requests

Counting the number of requests entails adding the voluntary or court-mandated requests or orders received by an organization, as appropriate for each of the types of reporting categories.

Number of subscribers/accounts/customers affected

It is possible that a single request might affect multiple subscribers, or accounts, or customers. A single order might name or otherwise identify each of the subscribers, or accounts, or customers or include an 'identifier' – a piece of data that is then used by the organization to subsequently identify the subscribers, or accounts, or customers associated with the request. When preparing their reports, organizations should tabulate all of the subscribers, or accounts, or customers affected by each of the types of reporting category requests.

Number of requests rejected

Organizations may sometimes reject requests for information that are made by government agencies. Rejections might be on the basis of improper request formats, on the basis of refusing to provide information absent a court order, or on the basis of other process or legal grounds. When preparing their reports, organizations should tabulate all of the legal or voluntary requests that they refuse, instead of tabulating the number of subscribers who would otherwise be affected by the request.

Number of requests contested

Organizations may sometimes dispute the requests that they receive from government agencies as a result of improperly scoped legal requests, on the basis of erroneous legal authorities being used to compel data from an organization, or on the basis of doubts concerning the legality or constitutionality of the request. Organizations should count each request they contested, as opposed to tabulating the number of subscribers/accounts/customers who are affected by the initial request and subsequent contestation.

Number of requests for which the organization has no data

Government agencies may sometimes make requests or demands for information where the organization does not possess any relevant information. Organizations should count each request for which they lack data, as opposed to tabulating the number of subscribers, or accounts, or customers who would be affected by the request but for whom the organization possesses no relevant data.

Number of requests for which partial information disclosed

Government agencies may sometimes make requests or demands for information where the organization possesses only some relevant information. Organizations should count each request for which they partially possess data, as opposed to tabulating the number of subscribers/accounts/customers who would be affected by the request but for whom the organization only partially possesses data.

Number of requests for which information is fully disclosed

Government agencies may sometimes make requests or demands for information where the organization fully discloses the requested or demanded information. Organizations should count each request for which they fully disclose data, as opposed to tabulating the number of subscribers/accounts/customers who are affected by the disclosure.

Number of users notified

Government agencies' requests will often affect a series of an organization's subscribers, customers, or users. Sometimes, though not always, organizations may notify those affected of the request. Organizations should count each affected person that they notify of the request; where they are barred from informing all those affected an organization might denote that either with a footnote associated with the reported number or in the narrative section of the report.

Narrative

Organizations may want to provide additional data concerning the requests that they receive from government agencies. The narrative, or descriptive, section of their report might explain some of the federal or provincial statutory powers that were used to compel information from organizations, any public court challenges where an organization is trying to narrow a government request, or explanations for why some information was provided voluntarily to government agencies. This section might also discuss whether users are notified of government requests and, if not, why not all persons are notified. It might also include, or link to, an organization's government requests guideline.

Organizations may also include contact information with their government requests report, so that customers and subscribers can contact the organization to provide feedback on how, why, and how long data is retained.

Furthermore, this non-structured information might include licensing information (is the document copyrighted, protected under a Creative Commons license, etc.) as well as a FAQ that provides answers to common questions that readers of government requests guidelines might regularly ask the organization.

Generating a Government Requests Report Using the DIY Transparency Report Tool

See **Appendix II** for how to create a government requests report.

Possible Questions About Government Requests Reports

Q: There are more categories in this report than in those published by most other Canadian companies. Why?

A: We opted to adapt the category structure suggested by the federal government of Canada. The government's structure provides clarity concerning the specific types of requests that an organization receives and subsequently responds to.

Q: Why should my organization spend the time developing and publishing this kind of a report?

A: For most organizations they will receive very few, or no, requests from government agencies on a yearly basis. As such, it shouldn't take too long to actually produce one of these reports and, when published, they will assure users and subscribers that the organization has a process in place to professionally respond to and account for these requests should they ever be made.

Q: How long will it take to produce one of these reports?

A: It should take very little time to actual input information into the DIY Transparency Report tool and subsequently generate a government requests report. However, organizations will need to separately collect and analyze actual requests they receive from government agencies over the course of their reporting period; such separate analysis may take very little time if few or no requests are made, or a longer period of time if there are numerous requests from government agencies over the course of the reporting period.

Q: Won't publishing these reports upset government agencies?

A: The federal government of Canada has endorsed the development and issuance of these kinds of reports.

Q: Why really cares about these kinds of reports?

A: Both internal and external stakeholders are interested in these reports. Internally, they can clarify whether an organization's current policies – such as accepting requests to voluntarily disclose information – are appropriate in light of the number of requests being made each year. Externally, subscribers and users who's data may be affected

have an interest in understand the regularity at which their data is being requested, citizens have an interest in knowing how government agencies are using their lawful powers, and politicians in evaluating whether agencies' powers either need to be constrained or subject to statutory reporting requirements.

Q: How should I publish my organization's government requests report?

You may choose to include your government requests report as a link in your privacy policy, within your company's corporate social responsibility documents or strategy, or other public-facing sections of your organization's website where you post privacy-related information.

Q: Where are resources to learn more about government requests reports?

Appendix III of this document includes resources concerning government requests reports.

Conclusion

Organizations are increasingly expected to be careful and thoughtful stewards of their subscribers and users' personal information. Holistic transparency reporting practices are one way for responsible organizations to showcase their commitment to protecting and responsibly disclosing information to government agencies. The DIY Transparency Report tool helps small- and medium-sized organizations more easily generate these kinds of reports, thus reducing some of the friction entailed in research, developing, and publishing information about how a company retains data, is willing to disclose data to government agencies, and explain how often and for what reasons government agencies request information.

Government agencies have gained numerous powers to compel information from companies over the past decades but have not had corresponding requirements to record and publicly account for how routinely they use their powers, or the effectiveness of such powers. Organizations cannot determine their effectiveness in assisting investigations but they can help their subscriber and users, and citizens more broadly, understand how often lawful powers are exercised and how many persons they tend to affect. Moreover, by publishing how they receive and respond to different kinds of requests organizations can prove to their users and subscribers that they are responsible in addressing lawful requests for information, and make transparent what their often opaque statements about cooperating with law enforcement in privacy policies and terms of service documents really mean.

Canadian privacy legislation, combined with statements made by the federal privacy commissioner, support organizations which decide to produce each component of a holistic transparency report. Industry Canada has even gone as far as to offer an example and guide for producing a government requests/disclosure report. And several Canadian companies have been releasing aspects of transparency reports since 2014. By creating and publishing holistic transparency reports, an organization can demonstrate it is a leader on privacy and data stewardship, while also exhibiting its responsible handling of government access requests. Neither privacy nor security are zero-sum games, and holistic transparency reporting offers one way for organizations to demonstrate how a privacy-protective the organization is while simultaneously being responsible for helping to keep society safe and well ordered.

Appendix I – DIY Transparency Report Tool Installation Guide

The DIY Transparency Report tool application ("app") is easiest to run in a virtual machine on and end user's computer. The app can also run on a web server. This appendix outlines how to install and setup the app on the end user's own computer.

NOTE: There are several pieces of software that need to be installed before attempting to install the app. Furthermore, the command line is used to start up the application. Command line commands are denoted using boldface.

The following process has been tested on Macintosh computers running the El Capitan operating system.

Software Requirements

Please install (or update to the latest version) these applications and tools in the listed order:

1. Virtual Box (https://www.virtualbox.org)
2. Vagrant (https://www.vagrantup.com)
3. Vagrant plugins (install via command line):
    a. Hosts updater: **vagrant plugin install vagrant-hostsupdater**
    b. VB Guest: **vagrant plugin install vagrant-vbguest**
4. Ansible (http://docs.ansible.com/ansible/intro_installation.html)
    a. On Macs, Ansible is easiest to install using Homebrew (http://brew.sh/)
        i. Run: **brew install ansible**
5. Setuptools for Python: **pip install --upgrade setuptools --user python**
6. Optional: Git (https://git-scm.com/book/en/v2/Getting-Started-Installing-Git)

Installing DIY Transparency Report

Once the above requirements are met follow the below steps in order.

1. Download the files required to set up the app's virtual machine using Vagrant as well as the Ansible playbook used for automatically configuring the vagrant machine.
    a. The installation files can be found here: https://github.com/andrewhilts/diy-transparency
    b. The simplest way to obtain these files is using git: **git clone https://github.com/andrewhilts/diy-transparency**. You can also

simply download a zip file from the project page.

2. In the terminal, **cd** into the downloaded project's directory. You can have a look at the VagrantFile and change the virtual machine name or IP address if you wish.
3. Then, make two directories, "code-api" and "code-frontend".
4. In the "group_vars" folder, edit "all" on lines 7 and 11 to change the passwords for your database to your own passwords.
5. Then, run **vagrant up**.
    a. You may be asked to enter your administrator password (this is to set up a line in your hosts file so you can access the app at http://diy-transparency.local)
6. Let vagrant and ansible setup the app for you. This can take up to 20 minutes on some devices.
7. Once installation has completed, navigate to http://diy-transparency.local in your browser and start using the app.

NOTE: If you need to pause the virtual machine, run **vagrant suspend** from the project directory. Simply run **vagrant up** again to bring the app back online. You'll have to do the latter after every reboot of the end user's machine.

Appendix II – Creating a Holistic Transparency Report

To generate a holistic transparency report, an organization must first install a copy of the DIY Transparency Report tool application ("the app"). This appendix explains how to use the tool.

When you first access the DIY Transparency Report app, you'll be presented with the main screen shown in Figure 1.

Figure 1: DIY Transparency Report Main Screen

The main tasks that you can accomplish using DIY Transparency Report are Creating

Transparency Reports, Managing already created reports, Modifying and/or editing the underlying categories and data types that are used to generate the reports, and exporting your reports for eventual publication.

Create New Report

It is easy to get started on a new transparency report. Click the button “Create new transparency report” from the DIY Transparency Report main screen and fill out the form that you are then presented with.

- Author name
- Date range for report
- Report publication date

The date range indicates the time period that’s covered by the new report. If you wanted to create a report for 2015 you’d selected 2015-01-01 as the start date and 2015-12-31 as the end date. You would then click “Save changes”. Afterwards, you would be presented with options to start working on the three components that make up a holistic transparency report: the data retention guide, the government requests handbook, and the government requests report.

Creating a Data Retention Guide

Data retention guides make explicit how long your organization retains different types of information. DIY Transparency Report makes it easy to create a retention guide for your organization.

Select the categories of data that you collect, the specific types of data retained within those categories, and indicate for how long you retain them. You can add custom data types and data categories right in this interface. When adding custom data types we recommend that you also add a description to your data retention guide to provide some detail about your retention practices and policies.

You can save your work by clicking the ‘Save changes’ button at the top of the form.

> You can modify the descriptions of default categories by navigating to: Manage Report Setup >> Manage data retention categories >> relevant category and specific data types.

As an example, you might select that your organization does collect some transmission data and note that the retained information is just the time and date of communications. You could then select the period of time for which data is retained,

which is shown as 2 years in figure 2.

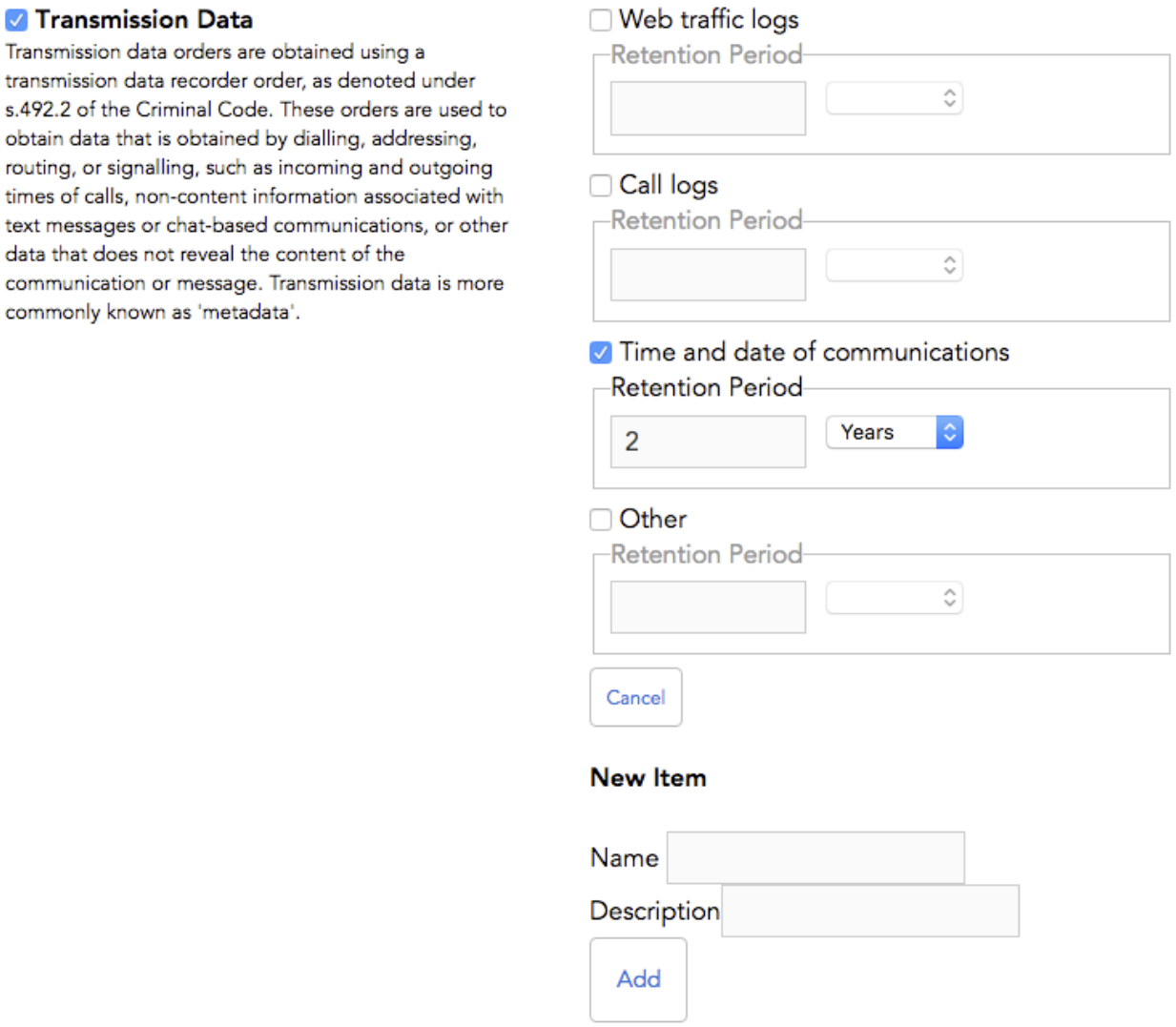

Figure 2: Screenshot from Creating a Data Retention Guide

When you are done inputting information into the data retention guide form, save your work and then click 'Back to report [number] overview'.

Creating a Government Requests Handbook

Creating a government requests handbook helps to clarify to law enforcement and the public the procedures you have in place to deal with requests for access to subscriber data.

You create a handbook by selecting the elements of the government request handbook that you want to include – such as your organization's policy on receiving

emergency requests, information on how you respond to international requests, or whether you notify users of government requests for their information – and the corresponding item with each category. You may add additional details to any of the options – such as providing information concerning your MLAT or user notification policies – by clicking on the '(i)' beside the relevant option.

You can save your work by clicking the 'Save changes' button at the top of the form.

> You can modify the descriptions of default categories by navigating to: Manage Report Setup >> Manage handbook categories >> Relevant category and specific data types.
>
> For the Government Requests Handbook, in particular, you may wish to add narrative information associated with each data type. Doing so will provide additional clarity on your organization's policies regarding interactions with government agencies.

As an example, you might select that your organization does have a policy concerning emergency requests, how you respond to international requests, and user notification. Figure 3 shows what it would look like to make such a selection.

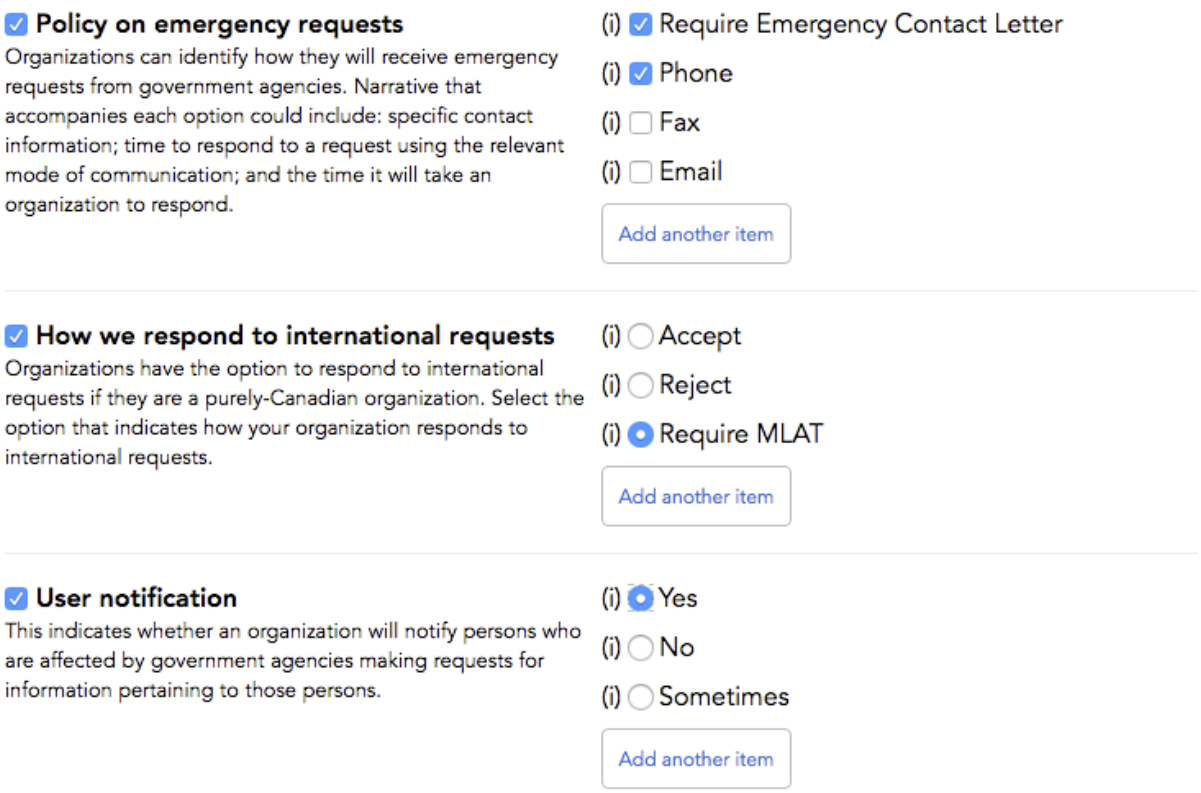

Figure 3: Making Selections to Create a Government Request Handbook

When you are done inputting information into the government requests handbook form, save your work and then click 'Back to report [number] overview'.

Government Requests Report

Creating a government requests report helps explain to the public how often, and on what grounds, government agencies request that your organization disclose data.

You create a government requests report by first collecting the requests that you have received over your reporting period and categorizing them. By default, the DIY Transparency Report app presents you with the categorization scheme we have adapted from the federal government of Canada. Once you have categorized the request – both by type, as well as numbers received per type and how the organization responded to the requests – you should identify the number of persons or accounts affected as well as the numbers of those affected your organization notified of the request. The aggregate of this categorization can be input into the table.

Your organization has the option of adding custom data types and data categories right in this interface. When adding custom data types we recommend that you also add a description to your government requests report to add some detail about the type or kind of request.

You can modify the descriptions of default categories by navigating to: Manage Report Setup >> Manage request categories >> Relevant category and specific data types.

You can modify the descriptions of the different request reporting categories (e.g. Subscribers notified) by navigating to: Manage Report Setup >> Manage request reporting categories >> Relevant category and specific data types.

Category		Number of requests (i)	Number of subscribers / accounts / customers affected (i)	Number of requests rejected (i)	Number of requests contested (i)	Number of requests for which the organization has no data (i)	Number of requests for which partial information disclosed (i)	Number of requests for which information is fully disclosed (i)	Number of users notified (i)
General Disclosures	Voluntary Disclosure at Organization's Initiative (i)	0	0	0	0	0	0	0	0
	Disclosures to Comply with Federal Law (i)	0	0	0	0	0	0	0	0
	Disclosures to Comply with Provincial Law (i)	0	0	0	0	0	0	0	0
	Disclosure in Emergency or Exigent Circumstances (i)	0	0	0	0	0	0	0	0
	Voluntary Disclosure Following Government Request (i)	0	0	0	0	0	0	0	0
	Add Type								

Figure 4: Example Screenshot of Government Requests Report

Figure 4 shows what a government requests report will look like before data is input.

When you are done inputting information into the government requests report form, save your work and then click 'Back to report [number] overview'.

Manage Existing Report(s)

You can examine all of your organization's reports in one list view. The list view provides information such as the time period the report covers, the time it was last updated, and whether or not the report has been marked as complete. There are also links to view/edit each report and delete the report if you'd like. You navigate to this by selecting either 'Manage transparency reports' from the Home screen or by selecting 'Reports' from the menu at the top of the screen.

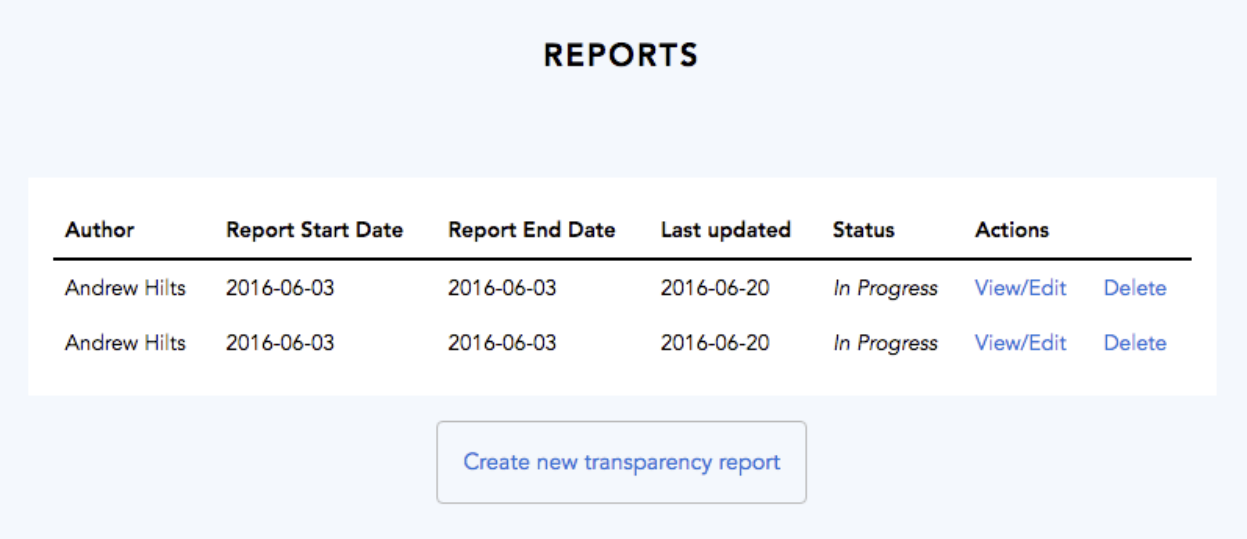

Figure 5: Screenshot of Manage Transparency Reports

You can mark your report as complete by clicking "View/Edit" and opting to include one or more report component (data retention guide, government request handbook, government requests report) into your final report. Your decision is registered by clicking the checkbox beside each component. Figure 6 shows what this will look like.

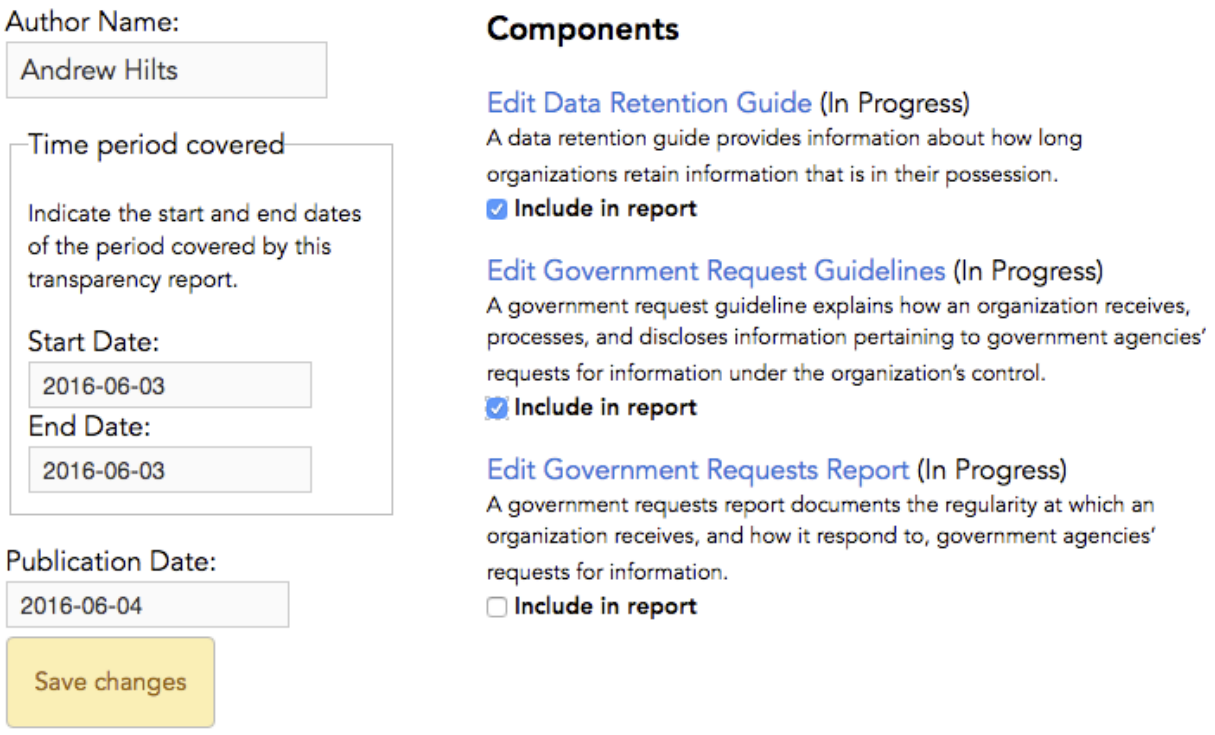

Figure 6: Selecting Report Sub-Types to Include in Holistic Report

Once you are satisfied with the state of each component you will need to navigate into

that component – such as the Government Request Guidelines that are currently in progress – and scroll to the bottom of that report. There, select the report as complete and click the "Save" button. Figure 7 shows what this will look like.

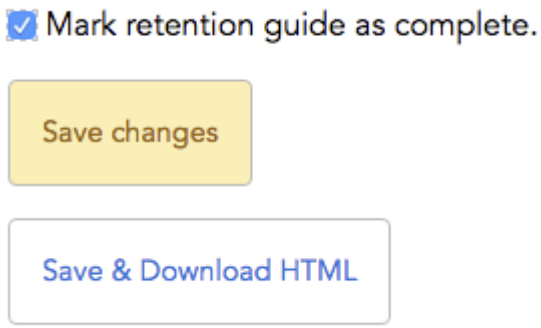

Figure 7: Marking a Report-Type as Complete

Once the component has been marked as complete you will see the option to Download an HTML or CSV version of the component in question, as shown in Figure 8. The process of downloading the component in question is discussed further in the next section.

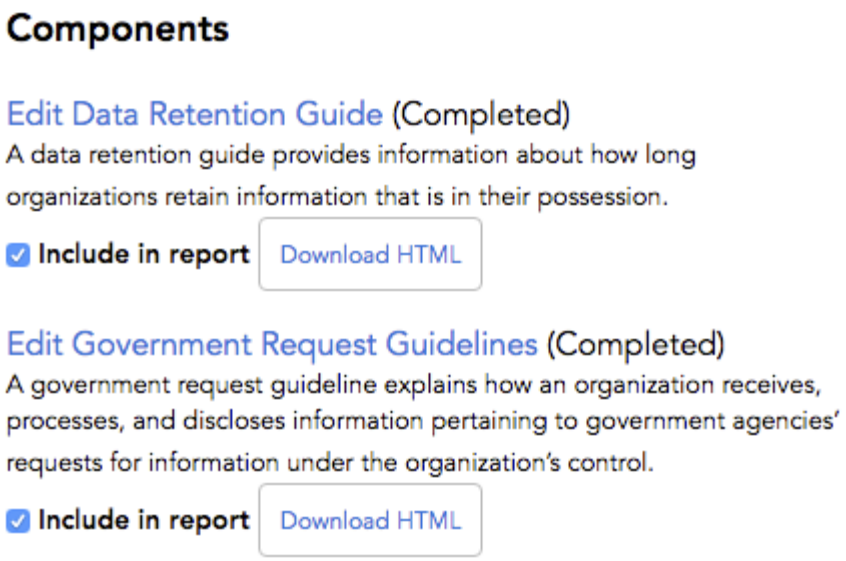

Figure 8: Downloading Completed Versions of Reports

Once all your included report components have been marked as complete, the report itself will be marked as complete when you navigate to 'Manage transparency reports'. This is shown in Figure 9.

Figure 9: Completed Reports in the Manage Transparency Reports Page

Export and Publish Report

DIY Transparency Report provides tools to help you develop and maintain your transparency reports. However, the system is designed to run internally, not as a public-facing website. As such, DIY Transparency Report provides you the ability to export your various report components for subsequent publication.

Each component can be exported as a basic HTML file, which you can then edit or style as you see fit. Additionally, the government requests report can be exported as a CSV for easy re-use.

Once you have marked a report component as complete, you can click a download button from the main report area. Otherwise, you can always download the in-progress report from the bottom of the component page itself.

Modifying Underlying Report Components

While you can add new data categories and types to your retention guide directly within the retention guide user interface, as well as the policies and options available for inclusion in your government request handbook in the handbook user interface, DIY Transparency Report includes handy report setup features where you can directly create, edit, and/or delete all the building blocks of your reports.

To access these features, click “Manage report setup” in the top-level navigation.

Data Retention Guide

Click on “manage data retention categories” to add/edit/delete categories included in existing and future data retention guides, and add/edit/delete the specific data types for each of those categories.

NOTE: When you add a new category or item in this area, they will not get added retroactively to existing reports. It is best to add new categories directly in the report interface. However, **if you delete a category or data type, they will be deleted from all pre-existing reports.**

Government Request Handbook

Click on “manage handbook guideline categories” to add/edit/delete the different law enforcement guidelines included in existing and future government request handbooks, and add/edit/delete the specific options for each of those guidelines.

NOTE: When you add a new category or item in this area, they will not get added retroactively to existing reports. It is best to add new categories directly in the report interface. However, **if you delete a category or data type, they will be deleted from all pre-existing reports.**

Government Requests Report

Click on “manage government request categories” to add/edit/delete the different categories of requests included in existing and future government requests reports, and add/edit/delete the specific request types for each of those categories.

NOTE: When you add a new category or item in this area, they will not get added retroactively to existing reports. It is best to add new categories directly in the report interface. However, **if you delete a category or data type, they will be deleted from all pre-existing reports.**

Click on “manage government request reporting categories” to add/edit/delete the different columns used to report values associated with each type of request. This is where you can add/edit/remove “number of accounts affected”, “number of requests rejected”, etc.

NOTE: When you add a new category or item in this area, they will not get added retroactively to existing reports. It is best to add new categories directly in the report interface. However, **if you delete a category or data type, they will be deleted from all pre-existing reports.**

Appendix III – Resources

Data Retention Guide

- Office of the Privacy Commissioner of Canada. (2014). "OPC Guidance Documents: Personal Information Retention and Disposal: Principles and Best Practices." Source: https://www.priv.gc.ca/information/pub/gd_rd_201406_e.asp.
- J. Warner. (2005). "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps." Source: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=777844.
- M. Geist. (2006). "The Risks and Rewards of Data Retention." Source: http://www.michaelgeist.ca/2006/01/the-risks-and-rewards-of-data-retention/.

Government Requests Handbook

- The 37th International Conference of Data Protection and Privacy Commissioners. (2015). "Resolution on Transparency Reporting." *Source:* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/15-10-27_Resolution_Transparency_Reporting_EN.pdf.
- C. Parsons and A. Molnar. (2013). "Law Enforcement Authorities Handbook Analysis." Source: http://catsmi.ca/resources/public-resources.
- Blizzard (World of Warcraft). (2009). "Law Enforcement Guide." Source: http://www.catsmi.ca/resources/public-resources.
- Foursquare. (2013). "Law Enforcement Data Requests." Source: http://www.catsmi.ca/resources/public-resources.
- Facebook. (2013). "Information for Law Enforcement." Source: http://www.catsmi.ca/resources/public-resources.
- Instagram. (2013). "Information for Law Enforcement." Source: http://www.catsmi.ca/resources/public-resources.
- LinkedIn. (2012). "Law Enforcement Data Request Guidelines." Source: http://www.catsmi.ca/resources/public-resources.
- MySpace. (2011). "Law Enforcement Guide." Source: http://www.catsmi.ca/resources/public-resources.
- Photobucket. (2010). "Law Enforcement Compliance Guide." Source: http://www.catsmi.ca/resources/public-resources.

- Tumblr. (2013). "Law Enforcement Guidelines." Source: http://www.catsmi.ca/resources/public-resources.
- Twitter. (2013). "Guidelines for Law Enforcement." Source: http://www.catsmi.ca/resources/public-resources.
- SaskTel. (2010, March 19). Customer Information Requests and Wiretap Services. SaskTel. Retrieved December 2, 2014, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.
- TekSavvy. (2014, June 4). Re: January 20 Data Request (items 1-10); May 1 Personal Information Template. TekSavvy. Retrieved December 12, 2014, https://citizenlab.org/wp-content/uploads/2014/06/TekSavvy-to-Citizenlab-2014-06-04.pdf

Government Requests Report

- The 37th International Conference of Data Protection and Privacy Commissioners. (2015). "Resolution on Transparency Reporting." *Source:* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/15-10-27_Resolution_Transparency_Reporting_EN.pdf.
- Geist, M. (2015, July 4). Telecom transparency reporting fails to satisfy. Toronto Star. Retrieved March 16, 2015, http://www.michaelgeist.ca/2015/07/telecom-transparency-reporting-fails-to-satisfy/.
- Google. (2016). Google Transparency Report: Requests for user information. Google. Retrieved March 15, 2016, https://www.google.com/transparencyreport/userdatarequests/?hl=en.
- Micek, P. (2016, revised Feb 18). Transparency Reporting Index. Access. Retrieved March 15, 2016, https://www.accessnow.org/pages/transparency-reporting-index.
- Rogers Communications. (2014b). Rogers Communications 2013 Transparency Report. Rogers. Retrieved December 14, 2014, http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf.
- Rogers Communications. (2015). Rogers Communications 2014 Transparency Report. Rogers. Retrieved March 15, 2016, http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf.

- SaskTel. (2014). SaskTel 2013 Transparency Report. SaskTel. Retrieved December 10, 2014, http://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES.
- SaskTel. (2015). SaskTel 2014 Transparency Report. SaskTel. Retrieved March 15, 2016, https://www.sasktel.com/wps/wcm/connect/a1a33ce6-ca5f-4077-ad67-44e9ebde3026/SkTel+Transparency+Report_Final+2014.pdf?MOD=AJPERES.
- TekSavvy. (2014, June 4). Re: January 20 Data Request (items 1-10); May 1 Personal Information Template. TekSavvy. Retrieved December 12, 2014, https://citizenlab.org/wp-content/uploads/2014/06/TekSavvy-to-Citizenlab-2014-06-04.pdf
- TELUS. (2014). TELUS Transparency Report 2013. TELUS. Retrieved December 13, 2014, http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf.
- TELUS. (2015). Sustainability Report 2015. TELUS. Retrieved March 15, 2016, https://sustainability.telus.com/wordpress/wp-content/uploads/2016/04/2015_Sustainability_Report-EN.pdf.
- Uber. (2016). Transparency Report. Uber. Retrieved April 15, 2016, https://transparencyreport.uber.com.