# Keeping Internet Users in the Know or in the Dark?

## The Data Privacy Transparency of Canadian Internet Carriers: A Third Report

**Jonathan A. Obar**

Department of Communication Studies, York University

jaobar@yorku.ca

**Acknowledgements**

The most important acknowledgement is to Professor Andrew Clement, whose vision for greater data privacy transparency in Canada began this project, and whose guidance and support makes continuing this work possible. I greatly appreciate the work over the years of IXmaps collaborators at York University and the University of Toronto: Antonio Gamba, Andrew Hatelt and Colin McCann. It is also important to acknowledge the input of Nate Cardozo (EFF), Steve Anderson, (Openmedia.ca), Christopher Parsons (Citizen Lab), Andrew Hilts (Cyber Stewards Initiative), and Tamir Israel (CIPPIC).

The methodology updated in 2014 and central to this third report was developed in collaboration with the Centre for Innovation Law and Policy at the University of Toronto. In particular, Matthew Schuman, Ainslie Keith, Shawn Arksey, Nathaniel Rattansey, Kassandra Shortt, Matthew Vaughan, Michael Cockburn, Caroline Garel-Jones, Jada Tellier and Aaron Goldstein.

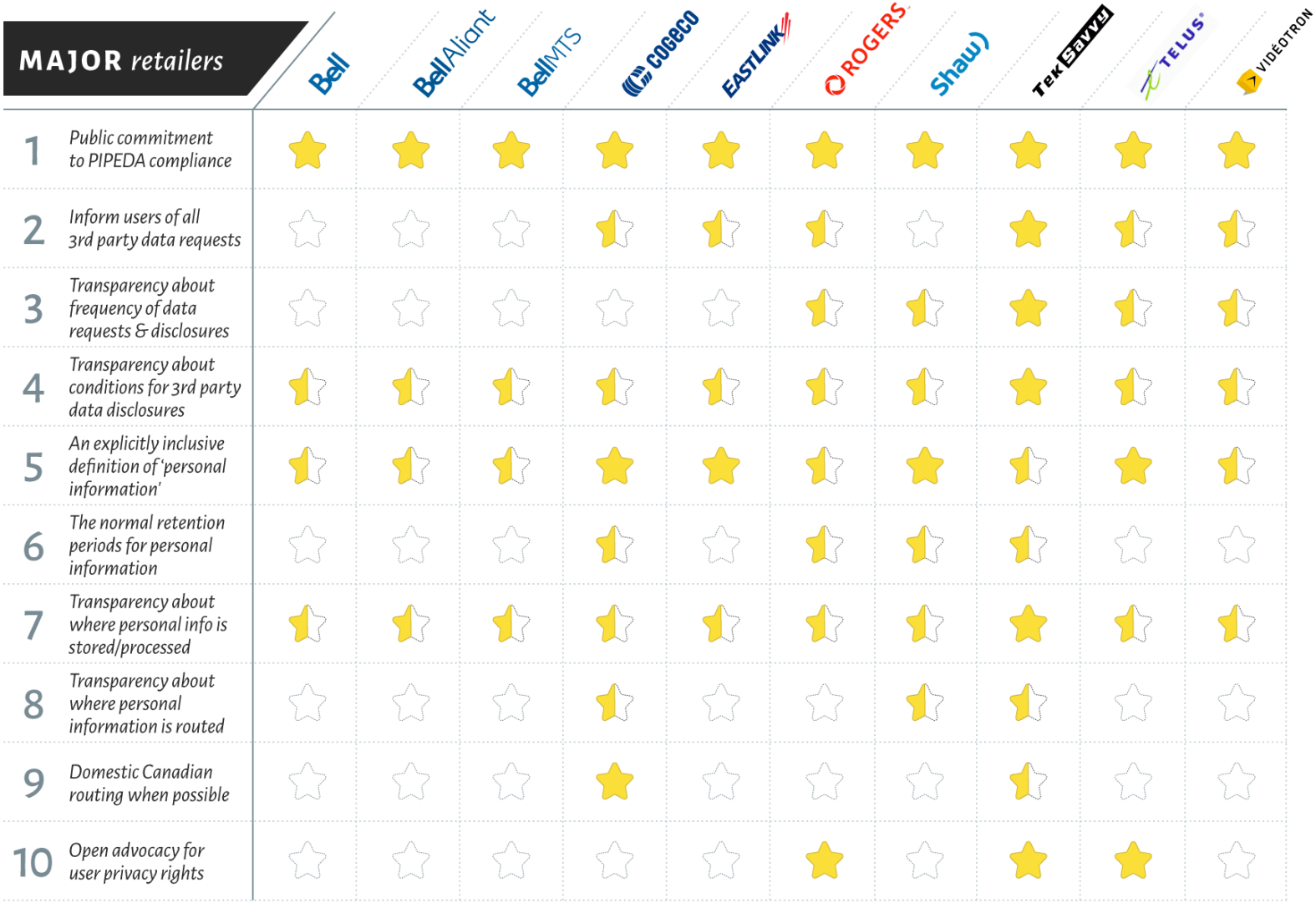
IXmaps website and design assistance: Jennette Weber

This third report is part of a broader effort associated with the *IXmaps: Mapping Canadian privacy risks in the internet 'cloud'* project (IXmaps.ca) and the Information Policy Research Program (IPRP) at the University of Toronto. Over the years, funding support for these reports has been provided by the Office of the Privacy Commissioner of Canada (2012-13), the Social Sciences and Humanities Research Council (2012-15), and the Canadian Internet Registration Authority (CIRA).

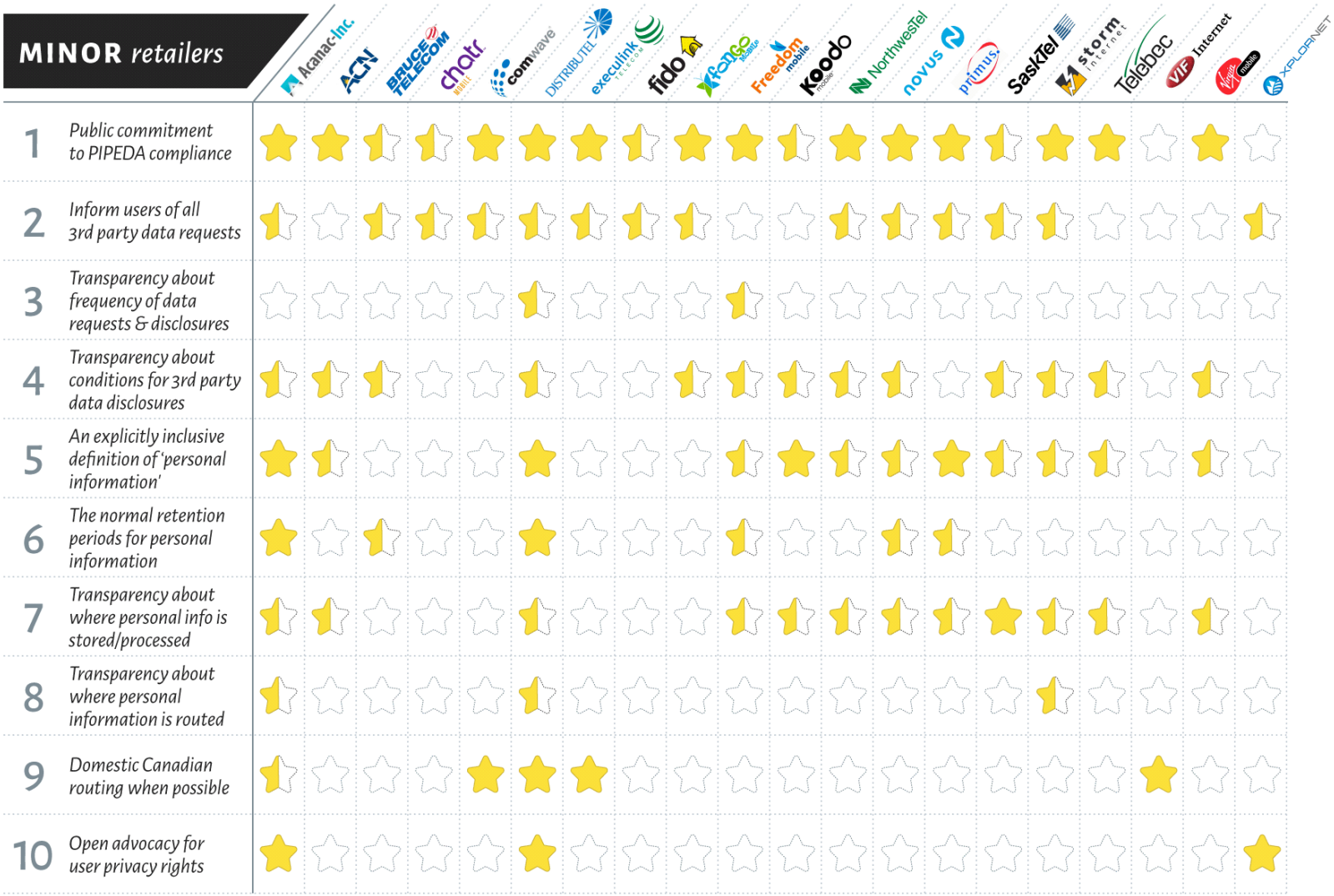
The views expressed in this report are the author's.

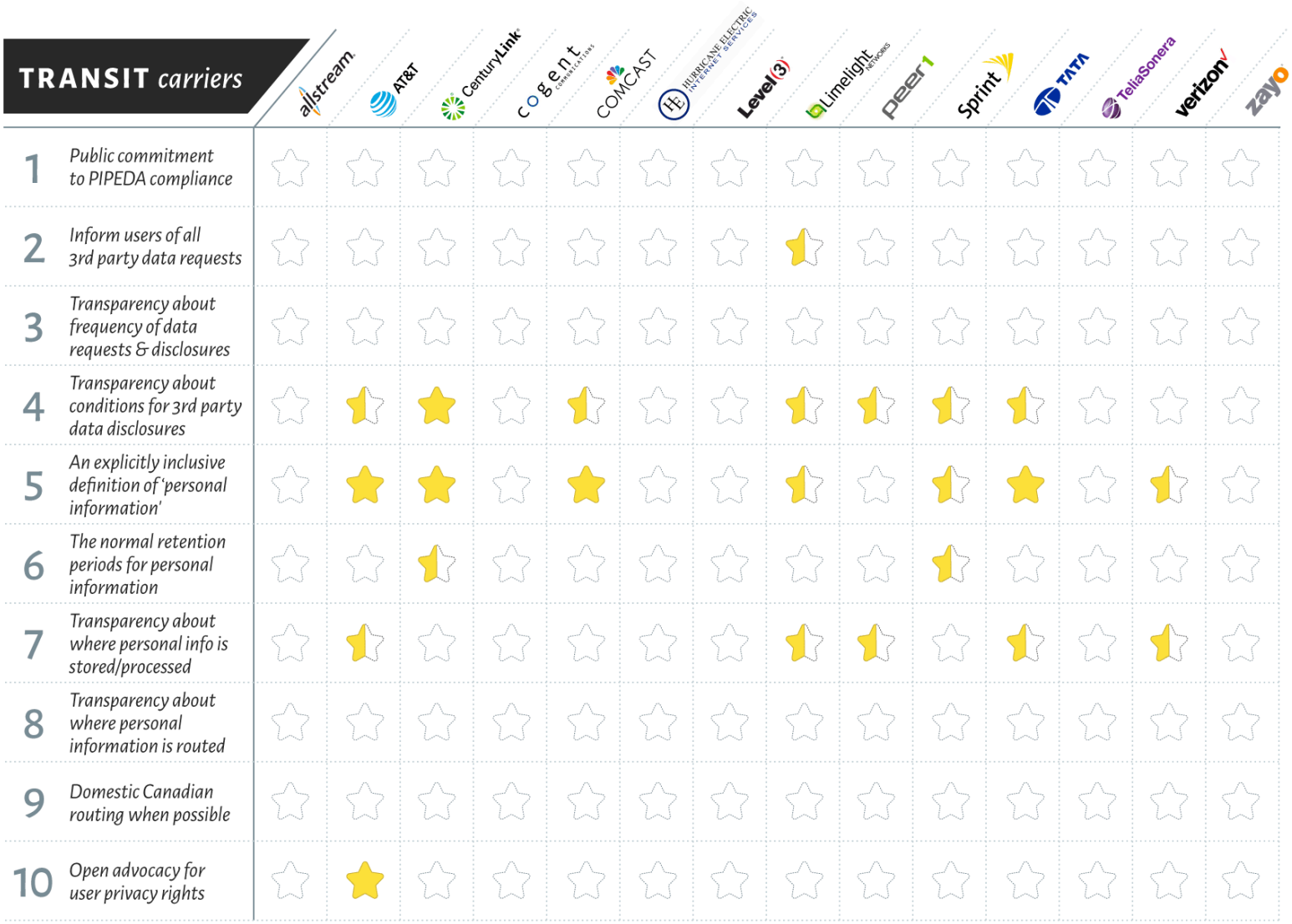


The report is available at: http://ixmaps.ca/transparency.php


MAJOR retailers
Bell
BellAliant
BellMTS
COGECO
EASTLINK
ROGERS
Shaw
TekSavvy
TELUS
VIDEOTRON
1 Public commitment to PIPEDA compliance
2 Inform users of all 3rd party data requests
3 Transparency about frequency of data requests & disclosures
4 Transparency about conditions for 3rd party data disclosures
5 An explicitly inclusive definition of 'personal information'
6 The normal retention periods for personal information
7 Transparency about where personal info is stored/processed
8 Transparency about where personal information is routed
9 Domestic Canadian routing when possible
10 Open advocacy for user privacy rights

## MINOR *retailers*




TRANSIT carriers
allstream
AT&T
CenturyLink
cogent
COMCAST
HURRICANE ELECTRIC INTERNET SERVICES
Level(3)
Limelight
peer1
Sprint
TATA
TeliaSonera
verizon
zayo
1 Public commitment to PIPEDA compliance
2 Inform users of all 3rd party data requests
3 Transparency about frequency of data requests & disclosures
4 Transparency about conditions for 3rd party data disclosures
5 An explicitly inclusive definition of 'personal information'
6 The normal retention periods for personal information
7 Transparency about where personal info is stored/processed
8 Transparency about where personal information is routed
9 Domestic Canadian routing when possible
10 Open advocacy for user privacy rights

**Keeping Internet Users in the Know or in the Dark?**
**The Data Privacy Transparency of Canadian Internet Carriers: A Third Report**

## Summary

This is the third report assessing the extent to which carriers providing internet communications in Canada are forthcoming about their handling of personal information. Demand for data privacy transparency calls our trusted internet carriers to account, for details about the collection, management, retention, routing, disclosure and use of our data. To what extent do carriers collect and keep personal information? Is data routed and stored in the U.S.? When a company, security agency or political party requests access to data, do carriers oblige? When it comes to these and many other privacy concerns, do our internet carriers keep us in the know? Or in the dark?

This report is being released at a time when governments and industries throughout the world struggle to improve online consent processes. Research suggests that users commonly ignore consent opportunities, in part, because they struggle with the mechanisms for consent facilitation which sometimes overwhelm with information, sometimes lack information, and sometimes encourage circumvention[1]. As consent is central to Canadian privacy law, solutions to the persistent challenge are needed[2]. As Commissioner Daniel Therrien advised Parliament in the Office of the Privacy Commissioner of Canada's 2016-2017 recommendations, "(Canadians require) better information to empower them to exercise individual control and personal autonomy. […] Individuals must be at the centre of privacy protection"[3].

What is clear is that the public trustee function that telecommunication providers operating in the public interest used to fulfill is more vital than ever. As privacy scholars and advocates call for information fiduciary and data trust models, Canadians should expect leadership from their internet carriers, especially the majors.

In response to these concerns, and in keeping with the principles of transparency and accountability that are fundamental to privacy law in Canada, this third report assesses the data privacy transparency of 44 major, minor and transit carriers that route Canadian internet traffic. Consistent with the previous reports, carriers are assigned full, half or zero 'stars' based on ten criteria:

*1) A public commitment to PIPEDA[4] compliance.*
*2) A public commitment to inform users of all third party data requests.*

---

[1] See: Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20.; Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media+ Society*, *4*(3); Oeldorf-Hirsch, A. & Obar, J. A. (2019). Overwhelming, important, irrelevant: Terms of service and privacy policy reading among older adults. *SMSociety '19,* July 19–21, 2019, Toronto, ON, Canada.

[2] See: Office of the Privacy Commissioner of Canada. (2016). Consent and privacy: A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act,* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

[3] Office of the Privacy Commissioner of Canada. (2017). 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/*

[4] Personal Information Protection and Electronic Documents Act.

3) *Transparency about frequency of third party data requests and disclosures.*
4) *Transparency about conditions for third party data disclosures.*
5) *An explicitly inclusive definition of 'personal information'.*
6) *The normal retention periods for personal information.*
7) *Transparency about where personal information is stored and/or processed.*
8) *Transparency about where personal information is routed.*
9) *Domestic Canadian routing where possible.*
10) *Open advocacy for user privacy rights.*

Stars were assigned after careful review of the privacy materials present in the privacy section of each carrier's corporate website as of January 2018. Materials not linked to a privacy section were not evaluated, as it is assumed that privacy pages are the first, and perhaps only location users interested in privacy will access[5].

The sample of 44 carriers involved in the routing of Canadian internet traffic was determined based on their prevalence in the IXmaps.ca traceroute database for the 2014 report. Most carriers are the same as in the 2014 analysis, with a few minor changes due to acquisitions, mergers and so forth. The sample includes 14 transit providers that are involved in the routing of traffic across the internet 'backbone', often via boomerang routes through the United States[6].

The star scores, or results for the ten criteria are organized into three star tables:

1 - Major Canadian retail internet carriers (see page 3)
2 - Minor Canadian retail internet carriers (see page 4)
3 - Major international internet transit carriers (see page 5)

The carrier ratings presented in this report are also available at IXmaps.ca/transparency.php.

**Key Findings**

While major concerns persist, there are clear signs that some carriers are moving toward greater transparency, providing more information about how they treat personal data. Table 1 emphasizes the bright spots, highlighting the scores of the 10 major carriers evaluated and the criteria that show the biggest improvements since the 2014 report.

The 2014 leader, TekSavvy, added an aggregate of 2 stars to achieve a score of 8/10, keeping it well ahead of all other major Canadian carriers. Shaw was the major carrier that showed the most improvement, more than doubling its score to 4.5. Cogeco and Videotron are others in this category whose scores rose considerably. Among the minor carriers, Acanac and its corporate owner Distributel stand out in both their scores and improvement from 2014.

---

[5] In the case of criterion 9 – *Publicly visible steps to avoid U.S. routing of Canadian data,* the peering arrangements identified on the website for TorIX, a Toronto-based internet exchange are also assessed.
[6] A boomerang route is an internet transmission that begins and ends in the same country, but goes via another. See: Obar, J. A., & Clement, A. (2012). Internet surveillance and boomerang routing: A call for Canadian network sovereignty. In *TEM 2013: Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association (Victoria)*; Clement, A., & Obar, J. A. (2015). Canadian internet "boomerang" traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In Geist, M. *Law, privacy and surveillance in Canada in the post-Snowden era*, 13-44, Ottawa, ON: University of Ottawa Press.

In terms of the criteria, the most notable improvements were associated with criterion 5: providing an explicitly inclusive definition of personal information. Four major and four minor carriers now earn full stars on criterion 5, whereas no major/minor carrier earned a full star in 2014. Modest improvements suggest some carriers are being slightly more transparent about the location of data storage (criterion 7) and data routing (criterion 8). These improvements may be due to demand for information about data sharing with the United States and corresponding surveillance implications. All major carriers now provide some level of detail about the location of data storage. In 2014 no carrier mentioned where data under their control might be routed, but now three carriers do so.

Table 1: Star scores and net improvements for major carriers since 2014

| Carrier | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Total | Net Improvement |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Bell** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Bell Aliant** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Bell MTS** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Cogeco** | 1 | 0.5 | | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 1 | | **5.5** | 1.5 |
| **Eastlink** | 1 | 0.5 | | 0.5 | 0.5 | | 0.5 | | | | **3** | 0 |
| **Rogers** | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | | | 1 | **5** | 1 |
| **Shaw** | 1 | | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | | | **4.5** | 2.5 |
| **TekSavvy** | 1 | 1 | 1 | 1 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 1 | **8** | 2 |
| **Telus** | 1 | 0.5 | 0.5 | 0.5 | 1 | | 0.5 | | | 1 | **5** | 0 |
| **Videotron** | 1 | 0.5 | 0.5 | 0.5 | 0.5 | | 0.5 | | | | **3.5** | 1.5 |
| **Net Improvement** | 1 | *-1* | 1 | 0 | 2 | 0.5 | 2 | 1.5 | *-0.5* | 0.5 | | |

**Almost all major carriers score above the average.** The average across the 10 majors was 4.2/10 stars, an increase from 3.5/10 in 2014.

**Bell remains the only major carrier to score below the 2.6/10 average with a score of 2.5 stars.**

**Bell receives no stars on the following criteria:**

*2) A public commitment to inform users of all third party data requests.*
*3) Transparency about frequency of third party data requests and disclosures.*
*6) The normal retentions period for personal information.*
*8) Transparency about where personal information is routed.*
*9) Domestic Canadian routing where possible.*
*10) Open advocacy for user privacy rights.*

While most major carriers in Canada are producing transparency reports, Bell Canada continues its refusal to release any details about law enforcement or third party requests or disclosures. In this respect, Bell demonstrates a disinterest in advocating for its customers' privacy rights and in its efforts to help users achieve meaningful consent. The other major carriers that have yet to release a transparency report are Cogeco and Eastlink.

**Minimum detail for minimum score:** While many carriers earned half-stars in a variety of categories, this should not be interpreted as a widespread overhaul of data privacy transparency practice. Many carriers scored half stars for the addition of a sentence or two or a brief example.

**No carrier earned a full star on the following criterion:**

*8) Transparency about where personal information is routed.*

**Only two carriers earned a full star on the following criteria:**

*4) Transparency about conditions for third party data disclosures.*
*6) The normal retention period for personal information.*
*7) Transparency about where personal information is stored and/or processed.*

**The 'fighting brands' of major mobile carriers, Chatr** (Rogers)**, Fido** (Rogers) **and Koodo (Telus), all score below the average and are less transparent than their corporate owners.**

**Carriers continue to refuse to provide retention details.** Despite growing calls for users to understand better how long carriers are keeping data, none of the major carriers, and few of the others, provide retention details, often noting that data will be kept as long as possible. This is frustrating, as some carriers do note that they maintain internal retention policies, but refuse to make these public.

**Many carriers continue to lack explicit definitions of personal information.** Despite some improvements in terms of the scores for this criterion, growing public concern about metadata, mobile data, surveillance data from in-store visits and set-top box data, is not reflected in the definitions provided by most carriers. Notable is the score of zero stars for Chatr (Rogers), Fido (Rogers) and Fongo in this category.

**No transit provider indicates explicit compliance with Canadian privacy law**. Since the first of these reports completed in 2013, not a single transit provider has made reference to Canadian privacy law in its privacy materials. This is concerning because these behind the scenes internet carriers handle large quantities of intra-Canadian traffic.

**Transit carriers generally score much lower than the retail carriers and typically expose personal data to mass state surveillance by the NSA.** All transit carriers (except for AT&T) score lower than the average. The following carriers earned a score of 0/10: Allstream, Cogent, Hurricane, Level 3, TeliaSonera and Zayo. This is concerning because when outside Canada, or handled by carriers subject to US or other jurisdictions, Canadian data enjoys no effective legal protection, and certainly much less than when within Canadian jurisdiction[7].

Given the lack of equivalent privacy protection between Canada and the US, the reliance on US transit providers or US routing for Canadian domestic internet traffic, aka 'boomerang' routing, it appears that **many Canadian internet carriers are in violation of their legal responsibilities under PIPEDA.**

**Overall, carriers continue to fail in their role as public trustees and as advocates for user privacy.** As government officials and privacy advocates call for new ideas and new mechanisms for protecting privacy, reputation and security, last-mile carriers, who deal with users face-to-face and/or online every month, must do far more. Transit providers too, must help ensure users

[7] Austin, L. M., Black, H., Geist, M., Levin, A., and Kerr, I. (2013 December 12). Our data, our laws, *National Post*, http://news.nationalpost.com/2013/12/12/our-data-our-laws/; Austin, L. M. (2015). Enough About Me: Why Privacy is About Power, Not Consent (or Harm), in Austin Sarat (Ed)., *A World Without Privacy?: What Can/Should Law Do,* New York, NY: Cambridge, 131-189; Austin, L. M. and Carens-Nedelsky, D. (2015). Jurisdiction still matters: The Legal Contexts of Extra-National Outsourcing, presented at the Assessing Privacy Risks of Extra-National Outsourcing of eCommunications public forum, *Seeing Through the Cloud: Why Jurisdiction Still Matters in a Digitally Interconnected World*, University of Toronto, March 6, 2015.

understand the processes and implications of going online. The consent challenges that persist epitomize current lackluster efforts. We cannot expect that content and platform providers will be the only entities helping to educate and engage users. Internet carriers must do far more to fulfill public interest mandates associated with longstanding expectations associated with the benefits of spectrum allocation, and certainly, the legal responsibilities determined by current privacy law.

**Primary Recommendation**

Our internet carriers must acknowledge and demonstrate a leadership role in the unfolding data privacy debate. Data privacy transparency means more than simply placing minimal text in a downloadable PDF on an almost hidden section of a website. Data privacy transparency should contribute to a more democratic and engaged discussion about the role of state surveillance in Canada and about the threats linked to corporate, political and governmental data collection, management, retention, disclosure and use. The presentation of comprehensive, meaningful and approachable privacy materials and transparency reports will help users to realize privacy rights, and also help to determine what additional regulatory and self-governance supports are necessary. This process should begin with our internet carriers serving as leaders in our efforts to try and control the unwieldy and complex big data universe. Secondary recommendations draw from the ten criteria assessed for this study, and are included in the full report.

**Keeping Internet Users in the Know or in the Dark?**
**The Data Privacy Transparency of Canadian Internet Carriers: A Third Report**

## Introduction

When we connect to the internet at home, at work, and on the go, our devices communicate with internet carriers. These companies, also referred to as ISPs (internet service providers) collect, manage, and retain our personal information as they facilitate the process of routing our communications. Unless we adopt special security measures, such as end-to-end encryption, our ISPs have full access to *all* the information we communicate over the internet.

While we knowingly interact with at least one internet company that sends us a bill every month, to ensure that our communication is sent where we want it to go, that company must communicate with a number of other carriers to achieve seamless communication from sender to receiver. Our online banking transfers, our Amazon purchases, our Twitter posts and our emails all require that data change hands, usually multiple times, as it is routed from our device to the server of the entity we're trying to reach and back. Along the way, every carrier has access to personal information about the communications it handles.

Providing personal information to these carriers, knowingly or unknowingly, introduces a variety of privacy concerns. For example, the role of corporate Big Data sharing and use in algorithmic decision-making, especially when automated eligibility determinations are made beyond our awareness, raises questions associated with sorting individuals and the forms of discrimination that may result[8]. The corporate world isn't the only context where privacy concerns are raised. Similar questions arise in the context of state-sponsored surveillance, especially as revealed by whistleblower Edward Snowden and others demonstrating widespread surveillance by entities like the U.S. National Security Agency (NSA) and Canada's Communications Security Establishment (CSE). As our last-mile and transit linkages to the network, our internet carriers place us in these problematic contexts, and also play a role through their own access to our personal information. Like Google and Facebook, internet carriers have a strong incentive to monetize the personal information they handle in such large volumes across all of our online activities, suggesting that these carriers potentially pose the biggest data privacy risk of all. If we are to maintain trust in these essential organizations, we need to know them much better than we currently do. They must be transparent and accountable.

To achieve this, there are many questions that require answering. To what extent do carriers collect our personal information? What types of information? Once they collect it, how long do they keep it? When a business, government or political party requests access to data, do carriers oblige? When they comply, do they inform users? Do carriers intensify privacy threats by routing data through the United States? Do they facilitate American capture of Canadian data, even when sender and receiver are both Canadian? In sum, when it comes to protecting our personal information, do our internet carriers keep us in the know? Or in the dark?

[8] See: Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. New York, NY: Routledge; Pasquale, F. (2015). *The black box society*. Cambridge, MA: Harvard University Press.

This is the third edition of a series of reports, originally titled "Keeping Internet Users in the Know or in the Dark?", assessing the data privacy transparency of the most prominent carriers that route Canadian internet traffic. One of the goals of these reports is to ease the burden faced by individuals living in Canada of determining the transparency of their internet carriers, and the extent to which those carriers appear to care about privacy. Similar to previous reports issued in 2013 and 2014, this report includes an evaluation of 44 carriers based on 10 standardized criteria. Carriers are awarded half or full stars on each. The results are presented in 'star tables' to reveal the carriers performing best, and to encourage carrier comparisons. Overall, the goal is that this research will support individuals living in Canada (and throughout the world) as they attempt to make informed decisions about the carriers they choose, where there is a choice, and to understand better the role carriers play in ensuring privacy protections. Should carriers score poorly, the hope is that users will raise concerns about lackluster approaches to user privacy as well as question the behaviour and the role of industry and government in changing it.

Background information on the reasons for assessing data privacy transparency is presented first. This is followed by a presentation of the study methodology – how carriers were chosen and evaluated. Results are presented next, which guide a variety of policy recommendations.

**The "Openness Principle" and Data Privacy Transparency**

The data privacy transparency concept draws from historical attempts to ensure users are adequately informed through notice when consenting to data collection, management and use. 'Notice' is a legal term that refers to efforts attempting to explain to users what will happen to data when it is provided to an external entity. Thus a notice component would be a communication tool, such as a privacy policy, for providing users with information about how their data is going to be collected and used. This particular tool would also ideally help users move towards meaningful consent to allow for lawful data practice.

The general guidelines for how this should be achieved date back at least to the formulation of the Fair Information Practice Principles (FIPPs), established in the U.S. in the 1970s, and updated by the OECD in the 1980s. Most relevant to the transparency concept is the OECD's "Openness Principle" stating,

> *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller*[9].

Since the FIPPs were integrated into the OECD's privacy guidelines, privacy law and policy has evolved throughout world, often drawing from the guidelines. Due to the central role of notice and consent to lawful data practice, openness is often provided primary emphasis. Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which governs commercial data use, is an exemplar in terms of this approach. PIPEDA has its own *Openness Principle* (PIPEDA Principle 8) stating,

> *An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information*[10].

[9] See: http://oecdprivacy.org/
[10] See: http://www.priv.gc.ca/leg_c/p_principle_e.asp

As the internet carriers involved in the routing of Canadian data engage in commercial data practice, the extent to which carriers satisfy PIPEDA's Openness Principle, operationalized here through ten data privacy transparency criteria, is evaluated.

**Assessing Transparency**

Consent is central to Canadian privacy law and fundamental to personal information protection[11]. If people don't have the information they need to make informed decisions, how can they protect themselves? How can they decide what to disclose online, which devices to use, when to complain or when to pursue legal action? How can we know when we need to encourage our carriers to change their practices? Or when the government needs to pursue change?

This study was conducted at a time when government and industry the world over are struggling with the implications of persistent consent failures. The literature suggests that it is a common for users to ignore digital consent opportunities[12], in particular, users often seem to agree to policies without accessing, reading or understanding them. Academic scholarship suggests a variety of reasons for this problematic behaviour, and one of them is the problem of notice[13]. As Commissioner Daniel Therrien noted in the Office of the Privacy Commissioner's 2016-2017 recommendations to Parliament "(Canadians require) better information to empower them to exercise individual control and personal autonomy. […] Individuals must be at the centre of privacy protection"[14].

These concerns are presented in the context of a problematic consumer choice model provided by PIPEDA, which largely places the burden of privacy protections on the user. In addition to the challenges associated with accessing and understanding privacy materials, which are sometimes "hidden"[15], PIPEDA requires that if individuals want to understand the data management practices of carriers, the individual must request their information, wait for the data, review, critique and respond. In light of the persistent consent challenge, this burden is extensive and unrealistic. This is hard enough with the ISP one deals with directly. But the task is made more difficult if one wants to learn how the other usually unknown carriers that route one's data handle

[11] See: Office of the Privacy Commissioner of Canada. (2016). Consent and privacy: A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act,* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

[12] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20.

[13] See: Cate, F. H. (2006). The failure of fair information practice principles. *Consumer protection in the age of the information economy*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972; Nissenbaum, Helen. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48; Solove, Daniel J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880-1903.

[14] Office of the Privacy Commissioner of Canada. (2017). 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/*

[15] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20; Obar, J. A., & Oeldorf-Hirsch, A. (2017, July). Clickwrap impact: Quick-join options and ignoring privacy and terms of service policies of social networking services. In *Proceedings of the 8th International Conference on Social Media & Society* (p. 50). ACM.

it en-route. This only begins to reveal to challenges associated with an evolving and highly complex internet industry, government security establishment and big data universe.

The growing challenges users face emphasize that the public trustee function that used to be central to telecommunications operation in Canada is needed now more than ever. Whether we move toward carriers serving as information fiduciaries, data trustees, or newer versions of public trustees operating in the public interest, what is clear is that to earn our trust, internet carriers will need to do a lot more to ensure that users can realize the privacy protections central to the spirit of Canadian privacy law.

Similar to the 2013 and 2014 reports, this third iteration employs a public accountability approach in assessing the publicly available privacy materials of 44 internet carriers involved in the routing of Canadian internet traffic. The analysis aims to highlight carriers that go beyond the letter of the law, and exemplify the spirit of PIPEDA's openness principle, through their data privacy transparency. The aim is to assist users in distinguishing between carriers to identify those genuinely interested in helping individuals living in Canada realize privacy protections.

Though this project was the first to assess the data privacy transparency of Canadian internet carriers with such a broad scope, it draws from a variety of similar efforts in Canada and abroad. Most notably is the Electronic Frontier Foundation (EFF)'s 'Who Has Your Back' reports[16] and the 'Ranking Digital Rights' Project[17]. Both projects involve transparency assessments of internet carriers in the United States and around the world utilizing a variety of criteria. This project borrows the EFF's 'star table' model most directly. It also complements the carrier questionnaires and transparency report assessments of Christopher Parsons and Andrew Hiltz at the University of Toronto's Citizen Lab[18].

It should be clarified that this research does not assess the actual data practices of internet carriers. Indeed transparency is an essential component of privacy practice, and is central to ensuring public accountability; however, this project assesses what carriers say about data, not necessarily what they do. As a result, it is possible that those assessed may be doing more to protect data than they say, or less. As it is likely easier to post privacy materials than to enact them, and doing so brings reputational benefits, the absence of such policies suggests that protections don't exist.

[16] See: https://www.eff.org/who-has-your-back-2013
[17] See: http://rankingdigitalrights.org/
[18] Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/; http://ottawacitizen.com/news/internet-firms-play-coy-on-how-they-share-info-with-police-government Christopher Parsons (2015), Do Transparency Reports Matter for Public Policy? Draft report dated January 15, 2015, available at SSRN http://ssrn.com/abstract=2546032

## Methodology

The method of assessment, as with the previous reports, draws from the EFF's "Who's Got Your Back" annual report. This report continues to focus specifically on carriers involved in the routing of Canadian internet traffic, as opposed to the broader scope taken by the EFF of assessing the privacy transparency of various service providers, many of them content providers.

### Sample

The current sample includes 44 carriers, with most having appeared in both the 2013 and 2014 reports. Over the years, some carriers have changed names or have been purchased by other corporate entities, and the updated sample reflects this. As with each of the reports, carriers were selected not due to their prominence in the Canadian ISP marketplace, but as a result of their appearance in the IXmaps.ca traceroute database. This sampling procedure is not exhaustive, but allows us to more accurately determine the scope of prominent carriers involved in the routing of Canadian internet traffic.

The resulting sample includes the following ten major carriers: Bell, Bell Aliant, BellMTS, Cogeco, Eastlink, Rogers, Shaw, TekSavvy, Telus and Videotron. The sample includes the following 20 minor carriers: Acanac, ACN, Bruce Telecom, Chatr, Comwave, Distributel, Execulink, Fido, Fongo, Freedom Mobile, Koodo, Northwestel, Novus, Primus, Sasktel, Storm Internet, Telebec, Vif Internet, Virgin Mobile, and Xplornet. Also sampled are a variety of domestic and foreign transit providers that handle Canadian internet traffic as it flows across the internet backbone. This includes the following 14 carriers: Allstream, AT&T, CenturyLink, Cogent, Comcast, Hurricane Electric, Level 3, Limelight, Peer 1, Sprint, Tata, TeliaSonera, Verizon and Zayo.

### Reviewing Privacy Materials

The carriers earn stars based on ten criteria discussed in the following section. Similar to the previous reports, privacy sections of corporate websites were reviewed for the assessment. Mobile apps were not reviewed. Links to privacy materials found on the front page of corporate websites were followed to privacy sections. Some carriers included a link labeled "privacy" on the front page, while others used a term such as "legal". Once on the secondary page, only materials associated with privacy protections were assessed. Thus, privacy policies, FAQs about privacy, videos about privacy, transparency reports, materials for third parties interested in lawful access requests, codes of fair information practice, and so forth were included in the assessment. Terms of service, user policies and other materials not associated directly with personal information privacy were not reviewed. Any materials not linked directly to a privacy page were not evaluated. Presumably users will look to the privacy pages for information about personal information protection, and may not look any further. For this reason, for the current report the methodology was very strict about this aspect and materials assessed did not include items found using search engines or on other website sections[19].

Similar to the approach with the previous reports, all carriers assessed were emailed multiple times throughout the analysis. They were first emailed to provide notification of a third report.

[19] The sole exception to the exclusive focus on corporate privacy and related statements is in the case of criterion 9, as discussed below.

Once a preliminary analysis was completed, another email was sent providing each carrier with their provisional scores. If any scores were changed after the initial analysis, carriers were updated. At each point in this process, carriers were encouraged to provide feedback on methodology as well as scoring to ensure that the analysis was fair and accurate. A number of carriers emailed to confirm that they updated their privacy materials after the preliminary analysis. All privacy materials for all carriers were assessed for a final time during the first week of January 2018 to ensure that all changes were reflected in the final scores.

**Evaluation Criteria**

The ten criteria were originally modeled from the criteria included in the EFF's 2012 *Who's Got Your Back* report. For the 2014 report, the criteria were updated with the support of the CILP Volunteer Student Working Group from the University of Toronto Law School. Creating an exhaustive operationalization of data privacy transparency is challenging, and instead the focus continues to be a number of criteria that appear vital to user engagement in their own data privacy protection. In particular, emphasis is on criteria that address concerns in Canada associated with the ongoing 'lawful access' debate as well as the 'boomerang routing' of domestic internet traffic through the US[20].

For the current report the same ten criteria from the 2014 report were maintained to allow for longitudinal comparisons. To maintain consistency in the assessments, as well as in communication with the carriers across time, the operationalization of the criteria, specifically how to receive full, half or no stars, are presented verbatim[21].

The 10 criteria are as follows:

**1) A public commitment to PIPEDA compliance**

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the Federal law in Canada governing commercial data practices[22]. All of the internet carriers assessed by this study are required to comply with this legislation[23]. Criterion 1 evaluates the extent to which carriers express a public commitment to complying with PIPEDA.

**Full Star**: The carrier explicitly indicates that it complies with PIPEDA, or similar applicable legislation, and provides substantive details of its privacy obligations, including that it only transfers personal information to third parties that provide an equivalent level of protection.

**Half Star**: The carrier only vaguely states that it operates according to applicable legislation or doesn't mention third party PIPEDA-equivalent protection.

[20] See footnote 6.
[21] Criterion 9 and criterion 10 were modified slightly. In an effort to facilitate the strict approach of ensuring materials were only assessed from corporate websites, flexibility with identifying peering arrangements was reduced from reviews of all internet exchange point websites to TorIX only for criterion 9. The modification to criterion 10 clarified that materials should be on corporate websites. See notes 27 and 28.
[22] https://www.priv.gc.ca/leg_c/leg_c_p_e.asp
[23] Sasktel is an exception as it is a provincially-owned Crown Corporation provider and is governed by the provincial (Saskatchewan) *Freedom of Information and Protection of Privacy Act.*

**No Star**: The carrier makes no indication that it complies with PIPEDA or substantially equivalent privacy legislation.

**2) A public commitment to inform users of all third party data requests**

In Canada, internet users have the right to know whether their data has been shared with a third party. PIPEDA states that carriers are obligated to provide this information, upon request. This criterion not only evaluates current practice, but is meant to encourage carriers to act in the spirit of the OECD and PIPEDA 'openness' principles. Proactive notification would demonstrate leadership in the battle to educate the public about privacy in the big data context. This would also make the education process more realistic, shifting the burden of disclosure notification from the user, where technocratic barriers are considerable, to the carrier, where proactive notification should be viewed as a component of a public trustee mandate.

**Full Star:** The carrier clearly indicates that it will notify a user when it has received a third party request for the user's information, unless explicitly prohibited from doing so by law.

**Half Star**: A carrier does not indicate that it will notify users when it receives requests, however it indicates that users may send an inquiry in order to acquire such information.

**No Star:** The carrier makes no mention of how users may learn of third party requests for their personal information.

**3) Transparency about frequency of third party requests and disclosures**

This criterion assesses whether carriers have released transparency reports. The reports often contain information about data requests and disclosures from third parties. While it is likely that the most common requests will come from government, security agencies or industry, the possibility exists that requests might come from other entities including political parties. Some reports will detail requests from within Canada as well as from other countries. Reports may also take the opportunity to articulate the value of transparency to privacy protection and education of the public about privacy and security.

**Full Star:** The carrier has published, in an annual or semi-annual report or in some other form, statistics regarding*:*

- The number of requests from third parties, broken down by government (law enforcement, etc.), commercial and non-commercial entities.
- How many requests it complied with.
- How many accounts the requests applied to.
- How many disclosures of information there were.

**Half Star:** The carrier has published SOME information but leaves many important statistics out.

**No Star:** The carrier has published no information relating to these types of statistics.

**4) Transparency about conditions for third party data disclosures.**

This criterion assesses whether carriers are transparent about the procedures for facilitating data disclosures to third parties. This includes providing information about communication requirements between the third party and the carrier.

**Full Star:** (1) The carrier explicitly states the circumstances under which personal information will be disclosed to third parties. (2) It must make clear what standard must be met by the third party in order for this disclosure to be made (e.g. whether a warrant is required). (3) It must be clear whether or not a subscriber/user will be notified in the case that his or her information is disclosed to a third party and especially the specific conditions under which such information will be disclosed without consent.

**Half Star:** The carrier refers to some but not all of (1), (2) and (3) or is vague about them.

**No Star:** The carrier fails to indicate any of (1), (2), or (3).

**5) An explicitly inclusive definition of 'personal information'.**

This criterion aims to address the broadening construct of personal information and the efforts by carriers to be transparent about the various forms of data collected about individuals.

**Full Star:** The carrier **explicitly** states all forms of data that fall under 'personal information'. This should include subscribers/users' IP addresses, IMSI/IMEI numbers, or MAC addresses, as well as their userIDs, meta-data (e.g. who subscriber communicated with, when and where this communication occurred), browser history (pages accessed, date of access, location when accessed), personal account information, credit card information etc.

**Half Star:** The carrier only **implicitly** states forms of data included in a definition of 'personal information', and/or provides a definition which (a) incorporates a closed list of what constitutes personal information that (b) excludes one or more of IP addresses, IMSI/IMSEI numbers, MAC addresses, userIDs, meta-data, browser history, personal account information, or credit card information.

**No Star**: The carrier gives no definition of 'personal information'.

**6) The normal retention periods for personal information**

This criterion aims to address the contentious issue of data retention, or the length of time data is kept by a carrier. Building from criterion 5, considering the various types of data collected, it is expected that carriers will describe how different retention periods correspond to data type.

**Full Star:** The carrier discloses how long personal information is routinely retained for, specifying retention time periods for each data type.

**Half Star:** The carrier only states the retention period for limited types of information. For example, a company may state that it retains consumers' browsing history for 2 weeks, but provides no information on call log retention.

**No Star:** The carrier either provides no information on data retention periods OR provides a statement so vague as to not inform the consumer beyond what PIPEDA requires. For instance,

> *"[Our company] shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected"*[24].

**7) Transparency about where personal information is stored and/or processed**

This criterion assesses what carriers say about their treatment of data 'at rest', or the extent to which carriers are transparent about the physical location of facilities where data is stored and/or processed. This information is vital to user understanding about the privacy implications of choosing one carrier over another as it is possible that certain carriers will be more likely to send personal information to foreign countries. Once data is outside Canadian jurisdiction it loses protections under Canadian law and is exposed to additional risks. This is particularly troubling in the U.S. context. As the U.S. Constitution does not apply to foreign data and the Canadian Constitution cannot protect data in foreign lands, Canadian data that enters into the U.S. falls into what Austin[25] refers to as a "constitutional black hole". It also becomes more exposed to mass surveillance by the U.S. National Security Agency (NSA). This means that when data is sent to the U.S. for storage and/or processing, Canadian civil liberties are threatened.

**Full Star:** The carrier clearly indicates the storage and/or processing locations of user's data and whether data storage and/or processing has been outsourced to a foreign company. This should include whether data may be stored in, or otherwise subject to other jurisdictions, what those jurisdictions are, and what sort of disclosure such data may be subject to.

**Half Star:** The carrier only indicates that there is a possibility that data may be stored and/or processed subject to a foreign jurisdiction. No jurisdiction is noted or details are not provided.

**No Star:** The carrier fails to clearly indicate whether or not data may be stored and/or processed such that it may be subject to a foreign jurisdiction.

**8) Transparency about where personal information is routed.**

Whereas criterion seven addressed what carriers say about data at rest, this criterion addresses what they say about data 'on the move'. This criterion assesses the extent to which carriers are transparent about the geographic locations data is routed or sent on its way to and from the user. As with criterion seven, data entering foreign jurisdictions is a central concern as research suggests that approximately 25 percent of Canadian domestic transmissions are routed through the U.S. (referred to as "boomerang routing") on its way from sender to receiver[26]. This criterion should also help users understand whether carriers are disclosing relationships developed with

---

[24] This is taken from Bell Canada's privacy policy, and echoes PIPEDA. Several Canadian companies go no further than this.

[25] Austin, L. M. (2016). Technological tattletales and constitutional black holes: communications intermediaries and constitutional constraints. *Theoretical Inquiries in Law*, *17*(2), 451-485.

[26] See: Obar, J. A., & Clement, A. (2012). Internet surveillance and boomerang routing: A call for Canadian network sovereignty. In *TEM 2013: Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association (Victoria);* Clement, A., & Obar, J. A. (2015). Canadian internet "boomerang" traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In Geist, M. *Law, privacy and surveillance in Canada in the post-Snowden era*, 13-44, Ottawa, ON: University of Ottawa Press.

transit carriers, which should be viewed as an important opportunity for carriers to educate the public about the role of these carriers in data flows online.

**Full Star:** The carrier clearly indicates whether Canadians' personal domestic communication data might be routed through the United States or otherwise subject to foreign jurisdiction while in transit. It clearly indicates the geographical locations where domestic communication is routed and what jurisdictions it is subject to. Similarly, it indicates whether or not communications with third countries is subject to U.S. jurisdiction.

**Half Star:** The carrier is vague about the geographical locations or jurisdictional exposure of personal data routing.

**No Star:** The carrier gives no indication of the geographical locations or jurisdictions where personal data is routed.

**9) Domestic Canadian routing when possible**

Building upon the previous two criteria, this criterion assesses the extent to which carriers demonstrate publicly that they are taking steps to ensure routing of domestic traffic remains within Canadian jurisdiction where possible. Ideally this information will be presented on privacy pages in an attempt to, again, educate the public about the role of routing and transit carriers in the process of facilitating online communications. Flexibility continues with this criterion including the awarding of stars to carriers that peer unconditionally at one Canadian internet exchange point (TorIX), which suggests that efforts are being made to promote Canadian network sovereignty through prioritization of Canadian connections.

**Full Star:** The carrier clearly states on its privacy pages a policy of domestic Canadian routing when possible, and indicates the concrete measures it takes to achieve this goal. A carrier that verifiably peers openly at TorIX (Toronto Internet Exchange) will also receive a full star. Only Canadian carriers are eligible for a full star, as foreign carriers by definition subject the data they carry to non-Canadian jurisdictions.

**Half Star:** The carrier is vague about its policies for ensuring Canadian routing of domestic traffic and the measures it takes to ensure this.

**No Star:** The carrier gives no indication of any policy or concrete measures to promote domestic routing when possible, nor does it peer openly at TorIX[27].

**10) Open advocacy for user privacy rights.**

Privacy pages can do far more than convey information about privacy practices, they can also serve as a platform for carriers to make clear their position about the role of privacy in their everyday operations. This criterion assesses the extent to which carriers express support for user privacy rights. This pro-privacy stance should positively contribute within the past 5 years to at least one of the following:

- Public debates about privacy and/or surveillance;

[27] Only peering noted on the TorIX website was assessed. This is a slight modification from the 2014 assessment.

- Legislative initiatives addressing privacy or surveillance;
- The defence of privacy rights in judicial contexts; or
- Relationships with privacy advocacy efforts.

**Full Star:** The carrier makes clear reference on its privacy pages to its support for user privacy rights in at least one of the areas itemized above.

**Half Star:** The carrier has defended user privacy rights politically, in court or legislatively, and there is vague reference to this on their privacy pages[28].

**No Star:** There is no readily available public evidence that the carrier has taken a positive pro-privacy position in any of the above areas.

## Results

### A few carriers lead in demonstrating greater transparency

Comparisons between the 2014 and the current report indicate that a small set of carriers are becoming more forthright about their treatment of personal information. As noted in Table 1 (see also pages 3-5 for star score visualizations), TekSavvy increased its 2014 chart topping score by two aggregate stars to a current score of 8 out of 10. Shaw more than doubled its score, increasing an aggregate of 2.5 stars, with Cogeco and Videotron each increasing their scores by 1.5 stars. In fact, all major carriers (except for Bell) scored above the sample average of 2.6/10 stars.

Enhancements to data privacy transparency are also evident with several minor carriers. As noted in Table 2, Acanac and its corporate owner Distributel increased their scores to 6.5 and 7.5 stars respectively. This is particularly noteworthy as Acanac didn't earn any stars in 2014. Freedom Mobile also scored considerably higher compared to its previous score as Wind, gaining 1.5 stars, suggesting that privacy transparency might be linked to its rebranding efforts. That being said, transit carriers (Table 3), generally scored poorly and show no overall improvement in demonstrating transparency. Perhaps this is because these carriers are generally invisible to the people whose data they carry, and hence feel little public pressure to improve their practices.

Table 1: Major Carriers: Star scores and improvements since 2014

| Carrier | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Total | Improvement |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Bell** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Bell Aliant** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Bell MTS** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | *-0.5* |
| **Cogeco** | 1 | 0.5 | | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 1 | | **5.5** | 1.5 |
| **Eastlink** | 1 | 0.5 | | 0.5 | 0.5 | | 0.5 | | | | **3** | 0 |
| **Rogers** | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | | | 1 | **5** | 1 |
| **Shaw** | 1 | | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | | | **4.5** | 2.5 |
| **TekSavvy** | 1 | 1 | 1 | 1 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 1 | **8** | 2 |
| **Telus** | 1 | 0.5 | 0.5 | 0.5 | 1 | | 0.5 | | | 1 | **5** | 0 |
| **Videotron** | 1 | 0.5 | 0.5 | 0.5 | 0.5 | | 0.5 | | | | **3.5** | 1.5 |
| **Improvement** | 1 | *-1* | 1 | 0 | 2 | 0.5 | 2 | 1.5 | *-0.5* | 0.5 | | |

[28] This element of the criterion is a slight modification from the 2014 report to ensure that all assessments, except those in criterion 9, address items located on corporate websites.

Reviewing improvements to specific criteria, most notable were carriers' efforts addressing criterion five: an explicitly inclusive definition of personal information. Four major carriers and four minors earned full stars. This is a considerable increase in scoring as no major or minor carrier scored a full star in the previous reports. The number of major carriers receiving scores for issuing transparency reports (criterion 3) grew from three (2014) to five. Rogers, TekSavvy and Telus received scores for these reports in 2014 as well, while Shaw and Videotron are the new additions. Looking at the major carriers, small changes were also evident in transparency about data storage locations (criterion 7) as well as the routing of data (criterion 8). Every major carrier in the sample scored at least a half-star on criterion 7, suggesting that this may be a response to growing demand for information about which countries one's personal data may be stored in and the additional surveillance threats this may pose. In 2014 no major carrier provided information on data routing, but Cogeco, Shaw and TekSavvy now do. While the details provided are still sparse, it signals that some carriers are beginning to acknowledge greater demand for more information about where data travels.

Similar advances are being made with some of the minor carriers. As Table 2 notes, more carriers received scores on criterion 7 (storage) and criterion 8 (routing) than in 2014, and in particular, many more carriers now acknowledge their commitment to PIPEDA protections in their privacy materials (criterion 1).

**Overall, most carriers score poorly on data privacy transparency**

While there are clear signs of improvement, including an increase from 2.2 to 2.6/10 average star scores across all carriers between 2014 and the current analysis, overall the findings emphasize that most continue to demonstrate little interest in transparency. The score increases should not be overstated. Many represent the addition of bare minimum details, with carriers meeting very low bars for half-stars. For instance, any mention of a country in the context of a single sentence about data storage is enough to earn a half star. No details are required about the amount of data stored, or processed abroad, how many data centres there are, or the specific cities where data is stored. To earn a half-star on criterion 8 carriers merely have to refer to the concept of routing, with the few that do generally providing little detail about geographic locations or routing practices.

**A lack of leadership**

Carriers consistently refer to themselves online as Canada's 'biggest', 'largest' and 'best' carrier. For example, Telus advertises its "largest and fastest network"[29]; Rogers claims to be "Canada's largest wireless service provider"[30], Comwave says it is "Canada's largest independent communications company"[31] while Distributel claims to be "Canada's leading independent Internet service provider"[32] and Eastlink describes itself as "the largest family owned and operated telecommunications company in Canada"[33]. As carriers boast about leading in terms of selling the 'biggest' and 'best' to consumers, few seem interested in leadership as a public trustee of private data, or as a carrier with a privacy-forward vision.

[29] See: https://www.telus.com/en/on/mobility/network
[30] See: https://investors.rogers.com/2017-annual-report/
[31] See: http://www.comwave.net/about/
[32] See: https://www.distributel.ca/about-distributel/who-we-are/
[33] See: https://www.eastlink.ca/about.aspx

This lack of leadership is particularly apparent with Bell Canada, "Canada's largest communications company"[34]. As calls for transparency have grown louder in the six years since this project started, a number of carriers have seen their scores increase considerably, some releasing transparency reports, providing detailed definitions and discussions of personal information handling. Bell Canada has only increased its score by 0.5 stars since the 2013 report, and in the current analysis stands alone as the only major carrier to score below the overall 2.6/10 average with a score of 2.5 stars. Further emphasizing this poor performance is the average score across the other seven major carriers of 4.9/10, and the average across the minors, 2.9/10, with Bell scoring well below both averages.

Bell received no stars on the following criteria:

*2) A public commitment to inform users of all third party data requests.*
*3) Transparency about frequency of third party data requests and disclosures.*
*6) The normal retention periods for personal information.*
*8) Transparency about where personal information is routed.*
*9) Domestic Canadian routing where possible.*
*10) Open advocacy for user privacy rights.*

A notable reason for Bell's low score is its continued refusal to release a transparency report about third party disclosures. While most major carriers and some minors now release these reports, Bell, Canada's largest provider, refuses to provide any information about third party requests received or data disclosed. Cogeco and Eastlink are the other major carriers that have yet to release a transparency report.

Table 2: Minor Carriers: Star scores and improvements since 2014

| Carrier | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Total | Improvement |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Acanac** | 1 | 0.5 | | 0.5 | 1 | 1 | 0.5 | 0.5 | 0.5 | 1 | **6.5** | 6.5 |
| **ACN** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | 0.5 |
| **Bruce Tel** | 0.5 | 0.5 | | 0.5 | | 0.5 | | | | | **2** | 0 |
| **Chatr** | 0.5 | 0.5 | | | | | | | | | **1** | 1 |
| **Comwave** | 1 | 0.5 | | | | | | | 1 | | **2.5** | 0.5 |
| **Distributel** | 1 | 0.5 | 0.5 | 0.5 | 1 | 1 | 0.5 | 0.5 | 1 | 1 | **7.5** | 5.5 |
| **Execulink** | 1 | 0.5 | | | | | | | 1 | | **2.5** | *-0.5* |
| **Fido** | 0.5 | 0.5 | | | | | | | | | **1** | *-0.5* |
| **Fongo** | 1 | 0.5 | | 0.5 | | | | | | | **2** | 0.5 |
| **Freedom Mob** | 1 | | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | | | | **3.5** | 1.5 |
| **Koodo** | 0.5 | | | 0.5 | 1 | | 0.5 | | | | **2.5** | 1.5 |
| **Northwestel** | 1 | 0.5 | | 0.5 | 0.5 | | 0.5 | | | | **3** | 0 |
| **Novus** | 1 | 0.5 | | 0.5 | 0.5 | 0.5 | 0.5 | | | | **3.5** | 0 |
| **Primus** | 1 | 0.5 | | | 1 | 0.5 | 0.5 | | | | **3.5** | 0 |
| **SaskTel** | 0.5 | 0.5 | | 0.5 | 0.5 | | 1 | | | | **3** | 0 |
| **Storm Int** | 1 | 0.5 | | 0.5 | 0.5 | | 0.5 | 0.5 | | | **3.5** | 3 |
| **Telebec** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | 0 |
| **VIF Internet** | | | | | | | | | 1 | | **1** | 0 |
| **Virgin Mobile** | 1 | | | 0.5 | 0.5 | | 0.5 | | | | **2.5** | 1 |
| **Xplornet** | | 0.5 | | | | | | | 1 | | **1.5** | *-0.5* |
| **Improvement** | 4.5 | 0.5 | 0 | *-1* | 4.5 | 2.5 | 2.5 | 1 | 1 | 2 | | |

[34] See: http://www.bce.ca/aboutbce/bceoverview

Table 3: Transit Carriers: Star scores and improvements since 2014

| Carrier | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Total | Improvement |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Allstream** | | | | | | | | | | | **0** | 0 |
| **AT&T** | | | | 0.5 | 1 | | 0.5 | | | 1 | **3** | *-1* |
| **CenturyLink** | | | | 1 | 1 | 0.5 | | | | | **2.5** | |
| **Cogent** | | | | | | | | | | | **0** | *-0.5* |
| **Comcast** | | | | 0.5 | 1 | | | | | | **1.5** | *-1* |
| **Hurricane** | | | | | | | | | | | **0** | *-1* |
| **Level 3** | | | | | | | | | | | **0** | *-1.5* |
| **Limelight** | | 0.5 | | 0.5 | 0.5 | | 0.5 | | | | **2** | 0 |
| **Peer 1** | | | | 0.5 | | | 0.5 | | | | **1** | 1 |
| **Sprint** | | | | 0.5 | 0.5 | 0.5 | | | | | **1.5** | *-0.5* |
| **Tata** | | | | 0.5 | 1 | | 0.5 | | | | **2** | 0 |
| **TeliaSonera** | | | | | | | | | | | **0** | *-0.5* |
| **Verizon** | | | | | 0.5 | | 0.5 | | | | **1** | *-1* |
| **Zayo** | | | | | | | | | | | **0** | 0 |
| | | | | | | | | | | | | |
| **Improvement** | 0 | 0 | -2 | -2.5 | -0.5 | 0 | 0 | -1 | 0 | 0 | | |

**A lack of full stars**

No carrier earned a full star for criterion 8: transparency about where personal information is routed. Only TekSavvy earned a full star on criterion 2: a public commitment to information users of all third party data requests, and criterion 3: transparency about frequency of third party data requests and disclosures. Two carriers earned full stars on criterion 4: transparency about conditions for third party data disclosures (TekSavvy and CenturyLink), criterion 6: the normal retention period for personal information (Acanac and Distributel), and criterion 7: transparency about where personal information is stored and/or processed (TekSavvy and SaskTel).

**Most carriers still refuse to provide information about data retention**

While some advances are being made, overall, carriers generally say very little about how long they keep personal data. Some carriers, Distributel and Acanac in particular, are beginning to provide detailed breakdowns of how long different types of data are retained. Four major carriers, four minor carriers and two transit carriers received half-stars, meaning that less than a quarter of carriers earned stars in this category. For those earning a half-star, the low bar allowed for the mentioning of one example of a time period for a score (e.g. keeping logs for six months), as opposed to a detailed description of multiple forms of data and retention details. It should be added that some carriers noted in their privacy materials that they maintain detailed internal retention policies, but refused to make these public. For example, Eastlink notes "Eastlink has a records retention policy that specifies the length of time that records are maintained"[35], but does not provide any of these details in its privacy materials.

**Most carriers lack explicit definitions of personal information**

Despite being the criterion where the biggest advances are being made, many carriers refuse to provide details about the types of personal information collected beyond phrasing such as 'service and usage records'. Metadata, device identifiers, set-top box data, surveillance data from in-store visits and a growing list of data points fill the data centres controlled by carriers. While some carriers including Shaw and Telus are exemplars in this area, most carriers continue to refuse to

[35] See: https://www.eastlink.ca/Portals/0/About/Code_of_Fair_Information_Practices-Eastlink.pdf

provide the details necessary to convey to users how much and what types of data are being collected every day. Most notable are the minor carriers that scored zero stars in this category, which includes: Bruce Telecom, Chatr (Rogers), Comwave, Fido (Rogers), Fongo, VIF Internet and Xplornet.

**Carriers still refuse to provide proactive notifications**

The problematic consumer choice model, which requires that users contact carriers to find out if their data was requested or disclosed places an unrealistic burden on consumers. Across the six years that we've been conducting this research, carriers have continued to refuse to offer any assistance in this area. TekSavvy is the only carrier among the entire sample that suggests that they will contact users, noting: "When a court orders us to provide personal information, we tell you about it unless we have been ordered by law not to, and we follow up regularly to question whether non-disclosure orders ought to remain in force"[36]. No other carrier in the sample makes a similar claim, and some refuse to include clear language clarifying users have the right under PIPEDA to contact carriers for this information.

**Most 'fighting brands' continue to score lower than their corporate parents**

Chatr (Rogers) and Fido (Rogers) each earned one star, compared to the five earned by their corporate parent Rogers. Koodo (Telus) earned 2.5 stars compared to the five earned by Telus. Freedom Mobile (Shaw) earned 3.5 stars while Shaw earned 4.5. Virgin Mobile (Bell) earned 2.5 stars, which is the same score earned by Bell. Chatr, Fido, Koodo and Virgin Mobile all earned fewer stars than the overall average of 2.6 stars. Freedom Mobile was the only fighting brand to earn above the average.

**Transit providers still refuse to mention compliance with Canadian privacy law**

Across the six years since this project started, not a single transit provider has made any reference to Canadian privacy law. While this is concerning due to the prevalence of transit services in the routing of Canadian internet traffic, the lack of Canadian content in privacy materials suggests little interest in educating users about how the internet operates or the protections that exist. It should be added that the retail carriers Canadians knowingly pay every month seem equally disinterested in educating the public about the role of transit providers in the routing of traffic. Carriers fail to be transparent about their relationships with transit providers or about the role of transit providers in the everyday routing of traffic. This suggests further that internet carriers demonstrate little interest in a privacy-forward leadership position or vision.

**Transit providers continue to score considerably lower than retail carriers**

All transit providers, except for AT&T, score lower than the overall average of 2.6/10 stars. The following transit providers scored zero stars in the current analysis: Allstream, Cogent, Hurricane Electric, Level 3, TeliaSonera and Zayo. It is worth noting that carriers whose privacy materials only referred to website traffic automatically received a score of zero. It is possible that these carriers had additional privacy materials elsewhere; however, the methodology was strict in requiring that privacy materials be linked to a privacy section of the website. Whereas in years past stars were awarded for materials not linked directly to the privacy section, this time the method was less flexible which explains many of the score decreases identified in Table 3. The poor scores for Sprint and Verizon require some clarification. Both of these carriers have fairly

[36] See: https://teksavvy.com/policies/legal-stuff/privacy-faqs/

detailed and extensive privacy materials; however, both have made efforts to provide users not from the U.S. with international policies. While this is certainly a step in the right direction, the international policies were not as detailed as the general policies and materials. As this study is being conducted in the Canadian context, only materials written for users operating in Canada (i.e. the international policies) were evaluated.

The continuation of poor scores for transit providers across the six years we've been conducting this research suggests further a disinterest in privacy-forward leadership, especially in an international context. Canadians should be especially concerned that storefront carriers are not holding transit carriers to account as required by law, and that transit providers seem disinterested in respecting their Canadian customers. Reliance on foreign transit services contributes to 'boomerang routing' or the routing of domestic internet traffic through a foreign country. Considering the important role that transit providers play in the routing of our traffic, and the surveillance threats that are introduced by boomerang routing, it appears that many of our internet carriers are in violation of their legal responsibilities under PIPEDA.

## Conclusion

Overall, carriers continue to fail in their role as public trustees and as advocates for user privacy. As government officials and privacy advocates call for new ideas and new mechanisms for protecting privacy, reputation and security, last-mile carriers, who deal with users face-to-face and/or online every month, must do far more. The consent challenges that persist help reveal the lackluster efforts of the internet carriers. We cannot expect that content and platform providers will be the only internet entities called on to respect privacy and to help educate users of their rights. Internet carriers must become leaders in the battle for user privacy, with one clear starting point - ensuring users are in the know.

## Recommendations

When carriers keep internet users in the dark, it is challenging for individuals to engage with their own privacy protections, which includes holding carriers accountable. The following recommendations aim to encourage greater self-regulation on the part of carriers operating in Canada and around the world, as well as policy change that should help support efforts to achieve the privacy outcomes associated with notice policy. Given the lack of progress since this project began in 2013, the recommendations are similar to those presented in previous co-authored reports[37]:

### *Recommendations directed at internet carriers*

These recommendations draw from the ten criteria addressed in the study. They suggest that carriers should not only achieve compliance with current law, but aim to reify the spirit of the law, especially as it pertains to PIPEDA's *Principle 8 – Openness.* Carriers should commit to being more proactive in their data privacy transparency efforts, ensuring that the information associated with the ten criteria discussed herein is available and accessible to users in the privacy sections of their websites. This should include the following:

[37] For example, the 2014 report co-authored with Andrew Clement: https://www.ixmaps.ca/transparency/2014-report.php

### Recommendation 1: Commit publicly to compliance with PIPEDA

Carriers involved in the routing of Canadian internet traffic should convey publicly that they are committed to complying with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). A link to the Act should be provided for users wanting more information. An assurance that any other carrier involved in the routing process, transit carriers in particular, provide the same privacy commitment should also be made clear.

### Recommendation 2: Commit publicly to proactive notification about third party data requests

Similar to recommendation one, carriers should also commit publicly through statements in their privacy materials that they will notify users in a timely fashion when third party data requests have occurred, unless they are prohibited from doing so by law.

### Recommendation 3: Routinely provide transparency reports detailing requests for data and information disclosures

At least once a year, carriers should be publishing transparency reports. These reports should be clear about the third parties requesting access to data, and should clarify entity name, entity type (government, corporate, political and so forth), location, legal authority, and request details. Request figures including total number of requests, and accounts implicated should be clear. The number of disclosures should be included with similar detail, but should also clarify whether disclosures are complied with in full or in part. Justifications should be provided. Transparency reports should be easily accessible to the public and located on privacy sections of websites. Public education materials such as infographics and videos are encouraged.

### Recommendation 4: Make publicly available information about the process through which third parties, including law enforcement, request and receive user information

The process, including the conditions required, through which requests for information are made should be open to public review. Law enforcement handbooks are encouraged. While this is an appropriate place to begin, carriers should consider finding new ways to make this information both available and accessible.

### Recommendation 5: Expanding and clarifying the personal information definition to include all relevant data types, beginning with metadata (such as location and device identifiers), set-top box and in-store surveillance data

To support user understanding of the quickly expanding types of data collected, a more detailed and exhaustive list of data types should be provided. Jargon such as metadata should be explained.

### Recommendation 6: Make publicly available detailed information about retention periods

Carriers likely have internal retention policies for a variety of data types. This information, including justifications, should be made available and accessible for public review. The implications of data retention should also be made clear, especially as it pertains to one-time consent processes.

### Recommendation 7: Clarify the extent to which user information is stored and/or routed outside of Canada

The legal jurisdictions where user data is stored and routed should be clarified. Country-level information should be provided at minimum. City-level information noting, for example, the location of data centres should also be provided. Carriers and data storage entities involved in these processes should be identified and the extent to which they comply with Canadian privacy law.

### Recommendation 8: Demonstrate efforts to ensure Canadian data remains within Canada

All strategies for ensuring that data generated in Canada is protected by Canadian law should be made accessible and understandable. Efforts to ensure that Canadian-to-Canadian transmissions are kept away from the United States, in particular, should be noted. Strategies might include: Canadian data storage, peering at Canadian IXPs (internet exchange points) that are public, handing-off traffic to entities that ensuring compliance with Canadian privacy law, and data encryption both when data is on-the-move and at-rest.

### Recommendation 9: Clarify how carriers work to protect internet users against government surveillance in Canada

As permitted by law, carriers should make clear the extent to which they have data sharing relationships with the Canadian government. How this relationship contributes to state surveillance, the justifications for this surveillance, and measures taken to ensure accountability and oversight should be made publicly available.

### Recommendation 10: Convey privacy advocacy position

Each carrier should make public its stance on advancing user privacy rights. This should include its position on alleged surveillance by the U.S. National Security Agency (NSA) and Canada's signals intelligence equivalent Communication Security Establishment (CSE). Lobbying efforts in support or in opposition to relevant legislation, regulation, and/or any advocacy efforts should be made clear. Any other legal proceeding that further conveys this position should be mentioned as well.

### Recommendation 11: Ensure that all privacy materials are accessible and user-friendly

All privacy materials should be consolidated and organized onto an easily accessible and understandable privacy section of the carrier's website. Links to this privacy section should be made available and clear and efforts to direct users to those links should be made. Individuals should not have to perform their own searches to locate these materials, including transparency reports, advocacy positions and law enforcement materials. Language should be simplified and consistent across materials. Infographics, videos and even gamifications are encouraged.

***For Provincial and Federal Privacy Commissioners as well as the Canadian Radio-Television and Telecommunications Commission (CRTC)***

### Recommendation 12: Relevant regulatory entities should engage in data privacy transparency oversight of all carriers involved in the routing of Canadian internet traffic

To ensure that both the letter and the spirit of Canadian privacy law (including the Telecommunications Act) are enforced, privacy commissioners and the CRTC must do more to help hold internet carriers accountable. This involves expanding and enhancing oversight efforts to ensure that "Canadian law governs Canadian data"[38]. Carriers must be held accountable if they refuse to do more to reduce boomerang routing, and also if efforts are not made to ensure transit providers comply with the standards set by the Canadian law.

***Recommendations for legislators***

### Recommendation 13: Amend *Principle 8 (the 'Openness Principle) of the Personal Information Protection and Electronic Documents Act*

As articulated in the 2014 report, PIPEDA's 'openness principle' should be amended to state:

> *An organization shall make readily available to individuals,* ***and the public generally****, specific information about its policies and practices relating to the management of personal information.* (emphasis added)[39]

### Recommendation 14: Amend *Principle 9 (the Individual Access Principle) of the Personal Information Protection and Electronic Documents Act*

One of the challenges central to current approaches to delivering privacy protections in Canada is the requirement that users contact carriers to receive and review information about data management efforts, including third party requests and disclosures. PIPEDA's Principle 9 should be amended to reduce this burden placed on the individual user and instead, require that carriers notify users if an entity requests access to data. Exceptions should be as limited as possible, and clarified to ensure public approval.

***Recommendation for law enforcement***

### Recommendation 15: Security or law enforcement agencies in Canada must issue transparency reports about relationships with internet carriers

The same data privacy transparency responsibilities of internet carriers should also apply to the security and law enforcement agencies operating in Canada. These responsibilities must include proactive transparency reporting about data requests and disclosures, justifications and evidence of public benefit.

***In sum, this project reiterates its call to the carriers, legislators, regulators, security and law enforcement personnel tasked with protecting the personal information generated by Canadian internet traffic – remove any and all barriers limiting data privacy transparency. This can be achieved by implementing proactive approaches to more robust and user-friendly information about data collection, management, disclosure, retention and use. In so doing, Canada will demonstrate to the world its leadership towards ensuring the delivery of privacy protections in the spirit of Canadian privacy law.***

---

[38] Obar, J.A. and McPhail, B. (2018). Preventing big data discrimination in Canada: Addressing design, consent and sovereignty challenges. CIGI. https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty

[39] See: https://www.ixmaps.ca/docs/DataPrivacyTransparencyofCanadianCarriers-2014.pdf