

Defining and Assessing Data Privacy Transparency: A Third Study of Canadian Internet Carriers

JONATHAN A. OBAR¹
York University, Canada

Data privacy transparency is defined here via four components: (1) notice materials (e.g., privacy policies) ensuring meaningful transparency contributes to meaningful online consent; (2) reporting about data practice frequency; (3) digital policy literacy supports; and (4) transparency that is useful as well as useable. To further understanding of this conceptualization, a third assessment was conducted of privacy materials from websites for major, minor, and transit carriers that route Canadian Internet traffic. Results from the sample of 44 Internet service and transit providers suggest carriers continue to demonstrate little interest in data privacy transparency. Minimal details are provided about third-party data requests, disclosures, routing, processing, storage, or retention. Transit providers make almost no reference to Canadian Internet transit practices. The privacy details present suggest that carriers have little interest in leading efforts to inform and educate people about how the Internet works or about privacy implications of Internet use. This perpetuates meaningful online consent challenges, and the marginalization of data subjects in broader Internet governance debates.

Keywords: privacy, transparency, privacy policy, Internet service provider

Data privacy transparency is an information dissemination end whereby those attempting data practices (i.e., collection, management, analysis, use, sharing, retention, etc.) communicate connections between those practices and privacy frameworks, considerations, or implications. A successful attempt requires openness and honesty, but also that the dissemination be “useful and usable” (see Habib et al., 2020), especially for holding those with data power to account (see Ananny & Crawford, 2018). Data privacy transparency is defined here via four components: (1) notice materials (for example, privacy and terms of

Jonathan A. Obar: jaobar@yorku.ca

Date submitted: 2020-06-18

¹ Acknowledgments: Thank you to Andrew Clement for your considerable contributions to this research, and to Jennette Weber and Valeta Wensloff for the graphic design. Many have supported the IXmaps.ca project over the years. Specific to this study, thank you to Antonio Gamba, Andrew Hatelt, Colin McCann, and the Centre for Innovation Law and Policy at the University of Toronto. This project is connected to funding from the Canadian Internet Registry Authority, the Social Sciences and Humanities Research Council of Canada, the Office of the Privacy Commissioner of Canada, and York University.

Copyright © 2022 (Jonathan A. Obar). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at <http://ijoc.org>.

service policies) for ensuring “meaningful transparency” (see Suzor, West, Quodling, & York, 2019) contributes to “meaningful consent” online (see Office of the Privacy Commissioner of Canada [OPC], 2018, para. 1); (2) transparency reporting about the frequency of data practices relevant to privacy considerations; (3) materials supporting “digital policy literacy” (Shade & Shepherd, 2013, “The Digital Policy Literacy Framework,” para. 1) to teach about connections to related political economic, policy, and infrastructure questions; and (4) delivering a “useful and useable” (Habib et al., 2020) transparency whereby the dissemination is practical and accessible to help data subjects address information asymmetries and associated privacy challenges. This conceptualization is discussed in the Assessing Data Privacy Transparency section.

In the transparency context, openness means providing breadth and depth of information to ensure that relevant details are available. While varying degrees of openness might produce a pragmatic transparency, without honesty in the details and in the framing, the information, or a lack of it, might mislead or confuse. Furthermore, to achieve a “useful and usable” (Habib et al., 2020) data privacy transparency, attempts must address informational and technical divides between data subject and manager (Obar, 2015, 2016; Schudson, 2015), ensuring sensitivity to increasing asymmetries as industry speeds ahead. This is a considerable challenge because the selection of useful information and its presentation in a way that is usable is context-specific. Context will differ depending on the privacy issues unique to the data manager or subject.

Thus, data privacy transparency is more than just words; it requires facilitating something for those engaging with the words. To realize transparency deliverables, opportunities for auditing and controlling data practices must be reified, with the aim of achieving accountability (Ananny & Crawford, 2018).

One way to develop understanding about a concept like data privacy transparency, and to provide critique, is to investigate the extent of its presence in a specific context. The current study attempts this, providing a third assessment (Clement & Obar, 2014, 2016) of the extent to which prominent carriers (Internet/transit service providers) involved in the routing of Canadian Internet traffic present a form of data privacy transparency. This third iteration aims to provide a new assessment of the 44 carriers in the sample, and comparisons with the last assessment in Clement and Obar (2016), to highlight any improvements. Beyond this narrow assessment of one group of data managers, the intention is that this study serve as a basis for further reflection on the data privacy transparency concept. Although the results of a study of Canadian Internet carriers may have a limited audience, how results help unpack the state of data privacy transparency and its possibilities may be relevant to international efforts addressing the future of online consent-based oversight mechanisms as big data and artificial intelligence pervade. Achieving data privacy transparency is a considerable challenge both for those providing the information and for those using the information. This study is an empirical assessment of the former, specifically, for carriers that route Canadian Internet traffic. Assessments of the latter are beyond the scope of this study.

The next section provides a discussion of data privacy transparency in the Internet carrier context. Information about assessing data privacy transparency is presented next, followed by the study.

Data Privacy Transparency and Internet Carriers

Any time an individual connects to the Internet, the connection is facilitated by Internet carriers. Often referred to as Internet service providers (ISPs), these carriers route traffic from sender to receiver and back, and while doing so may collect, use, disclose, and retain personal information. Individuals may be aware of the ISP they pay each month, but unaware that ISPs communicate with transit providers to facilitate Internet connection. Each packet transmission from sender to receiver could involve a small or large number of handoffs between carriers, exposing individuals to a small or large set of potential data practices (Clement & Obar, 2015).

Figure 1 visualizes a set of packet handoffs between carriers, and how privacy threats might arise. Displayed is a list of handoffs for a packet sent from a computer at the University of Toronto to the website for the Ontario Student Assistance Program (a student financial assistance program). This packet traceroute was collected via the IXmaps.ca project, which supports the crowdsourcing and review of traceroutes to identify how Internet transmissions and associated privacy threats may occur. Though the transmission begins and ends in Canada, it transits via Cogent, an American transit provider. As a result, the transmission passes through New York and Chicago before returning to Canada. This is referred to as a "boomerang rout(e)" (Clement & Obar, 2015). While it is intuitive that a visitor to Google from Canada might send packets south of the border, less intuitive is that Canadian-to-Canadian transmissions between an individual in Canada and a Canadian institution would transit the United States. What's more, while one might suspect that Americans could be watching a border-crossing to visit Google, it might be surprising to find out that ISPs and even the U.S. National Security Agency (NSA) are collecting data about Canadian visits to Canadian online services. Research suggests that approximately 22%–25% of Canadian-to-Canadian transmissions transit the United States, including visits to websites for Canadian banks, government agencies, universities, cultural institutions, and beyond (Clement & Obar, 2015; Obar & Clement, 2013). Because NSA surveillance is suspected at various Internet exchange facilities in the United States (Clement, 2013), the handoff to Cogent raises privacy concerns, especially considering that, as Austin (2016) suggests, Canadian data receive no Constitutional protections (American or Canadian) when passing through the United States.

Traceroute id: **6896**

Origin: **M5S3G6**

Destination: **osap.gov.on.ca** [204.41.8.65]

Submitted by: **cdm**

Submitted on: **12/01/2011** 4:23:17 PM

<u>Hop</u>	<u>IP Address</u>		<u>Min. Latency</u>	<u>Carrier</u>	<u>Location</u>	<u>GeoPrecision</u>
1	142.150.148.0	II	1	Univ. of Toronto	Toronto ON	building level
2	128.100.96.2	II	1	Univ. of Toronto	Toronto ON	building level
3	128.100.200.210	II	1	Univ. of Toronto	Toronto ON	building level
4	128.100.200.217	II	1	Univ. of Toronto	Toronto ON	building level
5	38.117.74.225	II	119	Cogent	Toronto ON	city level
6	154.54.40.165	II	119	Cogent	Toronto ON	city level
7	154.54.43.166	II	127	Cogent	Toronto ON	city level
8	154.54.42.69	II	138	Cogent	New York NY	city level
9	154.54.31.6	II	138	Cogent	New York NY	city level
10	154.54.10.238	II	145	Cogent	Chicago IL	city level
11	154.11.6.70	II	166	Telus	Don Mills ON	city level
12	207.219.86.174	II	166	Telus	Toronto ON	Maxmind
13	206.177.64.164	II	166	-Reserved AS-	Toronto ON	Maxmind
14	206.177.64.97	II	191	-Reserved AS-	Toronto ON	Maxmind

Legend



-  NSA: Known NSA listening facility in the city
-  NSA: Suspected NSA listening facility in the city



Figure 1. University of Toronto > OSAP boomerang traceroute details via IXmaps (n.d.).

Carrier connections raise additional privacy concerns as well. One is the extent to which personal information might be integrated into broader big data ecosystems. Generally dependent on the extent of data-sharing agreements between ISPs and third parties, as well as data leakage concerns, data collected by carriers could be implicated in automated eligibility systems in use across the global economy, raising concerns associated with digital discrimination (see Marwick & boyd, 2018; Pasquale, 2015).

How might individuals protect themselves from these threats? Policy based on the notice and choice privacy framework emphasizes user consent as a means for delivering protections (Cate, 2006; OPC, 2016). This translates to carriers providing policy texts to review (i.e., privacy and terms of service policies) that should contribute to meaningful online consent processes (OPC, 2018). In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs this approach in the context of commercial data practice. For example, PIPEDA’s “openness principle,” emulating elements of an Organisation for Economic Co-operation and Development (OECD, 2013) privacy policy framework, states,

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. . . . Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable. (Personal Information Protection and Electronic Documents Act [PIPEDA], 2000, Section 4.8, para. 1, Section 4.8.1, para. 1)

The challenges associated with the individual being at the center of the big data ecosystem as both "perpetual data subject and overwhelmed privacy savior" (Obar & Oeldorf-Hirsch, forthcoming) are discussed elsewhere (e.g., Calo, 2012; Nissenbaum, 2011; Oeldorf-Hirsch & Obar, 2019; Solove, 2013). Indeed, providing individuals with endless complicated policy texts to read has yet to be proved as a pragmatic strategy for delivering protections (McDonald & Cranor, 2008; Reidenberg et al., 2015). Nevertheless, if access to information about the data practices of Internet carriers is viewed as an essential first step toward privacy protections, the extent to which carriers provide this information should be assessed. Should a "meaningful transparency" (Suzor et al., 2019) result, subsequent strategies for moving from meaningful transparency to meaningful online consent should be determined. Should a problematic form of transparency result, continued calls for more effective data privacy transparency should be championed.

Conceptualizing Data Privacy Transparency

Data privacy transparency is conceptualized here via four components.

1) Notice materials (for example, privacy policies for digital services) ensuring "meaningful transparency" (Suzor et al., 2019, p. 1526) contributes to "meaningful consent" online (OPC, 2018, para. 1): Notice policy based on Fair Information Practice Principles (Cate, 2006) requires that those abiding by the policy provide data subjects with information about data practices. Some of the information required by PIPEDA, for example, pertains to data collection, disclosure, use, and retention. This information is often presented via privacy policies. To ensure that notice realizes its function as "fundamental" to privacy protections (Federal Trade Commission [FTC], 1998), the information provided must not be ambiguous or overly technical. It must focus on issues and implications that are meaningful—thus, "meaningful transparency." While providing this information is not all that is required to overcome information and technical asymmetries, it should be a step in that direction.

2) Transparency reporting about data practice frequency: To move from abstractions to specifics and to help clarify implications, entities involved in data practice should disclose the extent of these practices and the relevance to data subjects. How this can be done effectively is a question without a clear answer; some question whether recent approaches have been effective (Parsons, 2019), while others organize "best practices" (Woolery, Budish, & Bankston, 2016). As methods for moving toward "useful and usable" (Habib et al., 2020) details are debated, what is clear is that the goal is to bring data practices to the surface. This could support attempts to move data subjects from members of "known" to

“knowing” publics to create “more reflexive and active publics” (Kennedy & Moss, 2015, p. 2). Speaking about data mining, and envisioning participatory models that might even suggest a “democratising” of data processes, Kennedy and Moss (2015) emphasize that “accountability would therefore mean requiring data-mining companies not just to *show* the public what they are doing, but to *tell* publics what they are doing, why, and with what effect” (p. 6; emphasis in original). Though the feasibility of flawed consumer choice models remains in question (Obar, 2019; Solove, 2013), encouraging data managers to disclose details such as how often practices occur and how many individuals are implicated might contribute to a useful form of data privacy transparency.

3) Materials that promote digital policy literacy: The digital policy literacy concept is “aligned with critical approaches to digital literacy, and emphasizes how the effective use of digital media involves learning and negotiating the policy processes, political economic parameters, and infrastructural affordances that shape technologies” (Shade & Shepherd, 2013, “The Digital Policy Literacy Framework,” para. 1). Teaching data subjects about digital systems would connect data privacy transparency to approaches that suggest transparency can address corruption (Ball, 2009), and support “observation (that) produces insights . . . to govern and hold systems accountable” (Ananny & Crawford, 2018, p. 974). Digital policy literacy differs depending on the data privacy context, but emphasizes that understanding what goes on behind the screens may contribute to protections.

4) Ensuring that transparency is “useful and useable” (Habib et al., 2020): The previous three components emphasize a useful transparency for realizing oversight. Usefulness and usability, however, extend to methods of communication, including the form of language (such as plain language) and interface design. Although research in these areas is vital to realizing transparency ends (Schaub, Balebako, & Cranor, 2017), usability is not a focus of the current study.

Assessing Data Privacy Transparency

The study methodology originally drew from the Electronic Frontier Foundation’s “Who Has Your Back” reports (Electronic Frontier Foundation [EFF], 2011). The EFF method involved qualitative assessments of privacy materials provided by companies involved in data practice. In the 2011 report, assessments were via criteria that included “tell users about data demands,” “be transparent about government requests,” and “fight for user privacy in Congress” (EFF, 2011; see Table, row 1). Companies that fully or partially met the criteria received a full star, half star, or no star score on each. Scores were organized into star tables so companies could be compared. In conversations with the EFF when the first Canadian project began, it was expressed that the use of stars was to convey results through a more encouraging approach, as opposed to just critique.

The current effort, and the previous IXmaps data privacy transparency studies, advances an approach similar to the EFF’s; including criteria and star tables, and communication with carriers about the studies. Drawing from the EFF’s approach, a select group of 10 criteria in the current study begins to operationalize data privacy transparency for carriers that route Canadian Internet traffic. The list is not exhaustive, but draws on the first three components of the data privacy transparency conceptualization: emphasizing notice requirements, transparency reporting, and digital policy literacy.

Methodology

Sample

There are 44 Internet carriers assessed in this third study of data privacy transparency, with most appearing in Clement and Obar (2016) to allow comparisons across time. Any sample updates from the 2016 version reflect name changes and mergers/acquisitions. The first report was a pilot study (Clement & Obar, 2014), and those results will not contribute to the comparison. When the sample was originally organized, carriers were selected based on how often they appeared in the IXmaps.ca database. As noted earlier in Figure 1, packet traceroutes collected identify primary ISPs involved as sender/receiver, but also other ISPs and transit carriers involved in the packet's trip from where it originated to where it terminated. The study continues the assessment of ISP and transit carriers because data subjects with digital policy literacy should engage with the privacy materials for the different organizations that route Internet traffic. While this approach to selecting carriers isn't exhaustive, it does identify prominent carriers that route Canadian Internet traffic.

The sample consists of 10 "major" Internet carriers: Bell, Bell Aliant, Bell MTS, Cogeco, Eastlink, Rogers, Shaw, TekSavvy, Telus, and Vidéotron; 20 "minor" Internet carriers: Acanac, ACN, Bruce Telecom, Chatr, Comwave, Distributel, Execulink, Fido, Fongo, Freedom Mobile, Koodo, NorthwesTel, Novus, Primus, SaskTel, Storm Internet, Télébec, VIF Internet, Virgin Mobile, and Xplornet; and 14 transit carriers: Allstream, AT&T, CenturyLink, Cogent, Comcast, Hurricane Electric, Level 3, Limelight, Peer 1, Sprint, Tata, TeliaSonera, Verizon, and Zayo. Major carriers are among the largest ISPs operating in Canada, and minor carriers tend to be smaller. Transit carriers may be of different sizes and provide transit service to help facilitate Canadian Internet communications.

Identification and Analysis of Data Privacy Transparency Materials

To allow for comparisons with Clement and Obar (2016), the approach to data privacy transparency material identification and analysis was repeated. The path to privacy materials began with the researcher visiting the front page of the carrier's website and often scrolling to the bottom to find a "privacy" or "legal" link to dedicated privacy sections. Only privacy-related materials were identified and assessed, including privacy policies, transparency reports, codes of fair information practice, information about lawful access requests, privacy FAQs, and other privacy materials. While other policies, such as terms of service, may include privacy-related materials, over the years, the methodology was designed to emulate a data subject's likely approach to finding privacy materials. It is assumed that individuals will access materials labeled "privacy" first, and perhaps only, when looking for privacy information. Content not on the dedicated page or linked to it was not assessed.² Consultations with Dr. Andrew Clement were conducted to ensure consistency with previous assessments. A final review of data privacy transparency materials took place in January 2018. It is important to note that this is a study of carrier transparency, not carrier privacy practices (beyond transparency). Thus, this is an assessment of what carriers say about their approach to privacy, as opposed to actual data practices.

² There is one exception with Criterion 9, discussed later.

Evaluation Criteria

To assess data privacy transparency, each carrier earned a score on 10 criteria. Assessments involved assigning carriers a full star, half star, or no star on each. The study included the same 10 criteria as the previous study to support comparisons across time, in order to see if carriers enhanced data privacy transparency since the previous analysis. To ensure consistent operationalization of each criterion in terms of how full, half, or zero stars are awarded, criterion titles and the text associated with scoring are presented verbatim from Clement and Obar (2016), identified by italics (pp. 306–313).

The 10 criteria are as follows.

1) *A public commitment to PIPEDA compliance*

PIPEDA governs commercial data practice in Canada (PIPEDA, 2000). The carriers in the sample must comply with this federal legislation.³ This criterion assesses whether carriers are transparent about PIPEDA compliance, which would convey a commitment to the law, while also notifying users about applicable legislation. This is relevant to the notice and digital policy literacy components of the data privacy transparency conceptualization.

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.

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*

PIPEDA requires that entities involved in commercial data practice, within Canadian jurisdiction, inform individuals, on request, if their data were disclosed to a third party. This criterion goes beyond this and assesses whether data privacy transparency extends to informing users proactively about requests received for their data. In addition to connecting to the first three components of the data privacy transparency conceptualization, this also suggests a proactive measure that might ease the burden placed on individuals to chase entities involved in data practice.

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.

³ One exception is SaskTel, a Crown Corporation. This means that the Freedom of Information and Protection of Privacy Act (1990–1991) of Saskatchewan governs its actions.

Half Star: The carrier does not indicate that it will notify users when it receives requests, however it indicates that users may send an inquiry 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 (data) requests and disclosures*

Third parties requesting and receiving data could include commercial organizations, government entities, law enforcement and other security agencies, political parties, and other entities. This criterion assesses whether carriers are transparent about the frequency of these requests and/or disclosures. Information of this type might be presented in transparency reports, posted to privacy sections of corporate websites. The hope is that this will help individuals understand if carriers are engaged in data-sharing practices, as well as what other entities across the world might be interested in user data and for what purpose.

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

- *The number of requests from third parties, broken down by government (law enforcement, etc.), commercial and noncommercial 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 information provided about scenarios where third-party data disclosures occur. The aim is to evaluate whether carriers provide users with information to support notice policy components and digital policy literacy to help individuals understand how easy or difficult it is for ISPs to share data.

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 (their) 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"*

The intention is to assess how well "personal information" is defined. As the amount and types of data continue to expand, to support notice efforts and digital policy literacy, individuals should understand what different types of data carriers can access.

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 user IDs, metadata (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/IMEI numbers, MAC addresses, user IDs, metadata, 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 suggests that carriers should clarify data types collected and how long each is retained. Relevant to both notice and digital policy literacy components, this criterion begins to assess the privacy implications of retention, given that data analyses can change over time.

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 two 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.⁴

⁴ In Clement and Obar (2016), the following example is provided from a version of Bell's privacy policy in place until early 2017: "[Our company] shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected" (Bell, 2017, p. 7).

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

Supporting notice and digital policy literacy components of data privacy transparency, this criterion aims to help individuals understand where data are saved, maintained, and analyzed, given that many carriers have data centers in non-Canadian locations.

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*

This criterion is central to notice components because individuals should be aware of how their information flows across the Internet. This may help individuals develop digital policy literacy about the Internet and about the privacy implications of "boomerang routing" (Clement & Obar, 2015).

Full Star: The carrier clearly indicates whether (data from Canada) . . . 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) *(Transparency about) domestic Canadian routing when possible*

This criterion assesses transparency about privacy-forward efforts to ensure Canadian routing of Canadian data, where possible. This criterion includes one exception to only assessing materials from carrier websites. Carriers identified as peering unconditionally at TorIX, a Toronto-based Internet exchange point, receive a star, because carriers doing so demonstrate publicly their commitment to reducing boomerang routing.

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.⁵

10) Open advocacy for user privacy rights

This criterion assesses whether carriers attempt to inform users about a privacy-forward commitment, which might help users realize not only that privacy is important, but also that carriers support and even fight for user rights.

Full Star: The carrier makes clear reference on its privacy pages (in the last five years) to its support for user privacy rights in at least one of the following areas:

- *deliberations or discussions about privacy or surveillance occurring in public;*
- *legislative, regulatory, or judicial contexts;*
- *privacy activism or advocacy.*

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.

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.⁶

Results

While a number of carriers made improvements since the 2016 analysis (Clement & Obar, 2016), overall, a robust data privacy transparency continues to be absent across the sample. This section begins with a description of the star scores from the current analysis. A comparison with the 2016 scores follows.

⁵ Whereas previously, peering arrangements at various IXPs were included, for the current assessment, only TorIX peering was considered.

⁶ Criterion 10 was modified to address dedicated privacy sections of websites only.

The average across the sample was 2.6/10 stars, while averages for the major carriers, minor carriers, and transit carriers were 4.2/10, 2.9/10, and 1.0/10, respectively. Of all 44 carriers, TekSavvy scored the highest, with 8/10 stars, earning six full stars. As noted in Figure 2, the three other majors with the closest scores were Cogeco (5.5), Rogers (5), and Telus (5). While the remaining majors scored fewer than five stars, none of the majors scored zero. The Bell companies (Bell, Bell Aliant, and Bell MTS) all received the same lowest score for the majors, 2.5/10 stars, and were the only major carriers to score below the sample average.

MAJOR carriers	Bell	Bell Aliant	Bell MTS	Cogeco	Eastlink	Rogers	Shaw	TekSavvy	Telus	Vidéotron
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	☆	☆	☆	☆	☆	★	☆	★	★	☆

Figure 2. Star table for major carriers.⁷

All majors received a full star on Criterion 1 (transparency about PIPEDA compliance), and full or partial stars on Criterion 4 (disclosure conditions), Criterion 5 (personal information [PI] definition), and Criterion 7 (storage/processing)—though only TekSavvy earned full on 4 and 7. Most majors scored half stars or no stars on the remaining criteria, with the fewest scores for 6 (retention), 8 (routing location), and 9 (domestic routing).

⁷ Figures 2, 3, and 4 and Tables 1, 2, and 3 were first posted on ixmaps.ca in "Keeping Internet Users in the Know or in the Dark? The Data Privacy Transparency of Canadian Internet Carriers: A Third Report."

Referring to Figure 3, many minor carriers scored poorly. Distributel (7.5/10) and Acanac (6.5/10) had the highest scores, though it should be noted that Acanac is owned by Distributel. No other minor carrier scored more than 3.5/10. In fact, 12/20 carriers scored below the minor carrier average of 2.9/10. Minor carriers scoring the lowest were Chatr, Fido, and VIF Internet, all with only one star. The criteria with the fewest scores in this group were Criterion 3 (transparency about requests/disclosures), Criterion 8 (routing location), and Criterion 10 (privacy advocacy).

MINOR carriers		Acanac	ACN	Bruce Telecom	Chatr	Comwave	Distributel	Execulink	Fido	Fongo	Freedom Mobile	Koodo	Northwestel	Novus	Primus	SaskTel	Storix Internet	Telebec	VIF Internet	Virgin Mobile	Xplornet
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	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★

Figure 3. Star table for minor carriers.

Referring to Figure 4, scores reveal that transit carriers also scored poorly. AT&T had the highest score, with 3/10, and was the only transit carrier to score higher than the overall sample average. CenturyLink scored 2.5/10 while Limelight and Tata scored 2/10. Allstream, Cogent, Hurricane, Level 3, TeliaSonera, and Zayo all received zero. Carriers that received zero may have had privacy materials located on different website sections. If privacy materials only referred to the carrier website and not to broader communication practices, zero was assigned. These issues did contribute to scores of zero with some transit providers.

TRANSIT carriers		Alstream	AT&T	CenturyLink	Cogent	Comcast	Hurricane Electric	Level 3	Limelight	Peer 1	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	☆	★	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆

Figure 4. Star table for transit carriers.

Clarification is necessary for Sprint’s and Verizon’s poor scores. Although both provide various privacy materials online, the presence of international policies specifically for non-U.S. users, and not the general privacy materials, were the items assessed for this Canadian-centric study. Both carriers should be commended for providing country-specific privacy materials; however, those materials should be as detailed and as clear as the materials for users accessing the Internet in the United States.

Across the sample, no carriers received a full star for Criterion 8 (routing location); TekSavvy was the only carrier to receive a full star for 2 (informing users about data requests), and 3 (transparency about requests/disclosures); CenturyLink and TekSavvy were the only carriers to receive a full star for 4 (disclosure conditions); Distributel and Acanac were the only carriers to receive a full star for 6 (retention); and SaskTel and TekSavvy were the only carriers to receive a full star for 7 (storage and processing).

Star Score Comparison With the 2016 Study

A comparison with the scores in the 2016 report (Clement & Obar, 2016) reveals that a small number of carriers in the sample are demonstrating greater data privacy transparency. The average score across the sample increased from 2.2/10 to 2.6/10 stars. The improvements noted in Table 1 demonstrate that TekSavvy increased by two stars, receiving the highest score in both studies. Other changes with the major carriers include Shaw, which increased its score by more than double, adding 2.5 stars, for a total score of 4.5/10. Vidéotron and Cogeco increased by 1.5 stars, with overall scores of 3.5/10 and 5.5/10, respectively. A review of all the major carriers reveals that five increased scores, Eastlink and Telus earned the same score, and the Bell companies were the only carriers to lose points (because of modified language in their materials, pertaining to Criterion 2).

One reason the Bell companies scored so poorly was the organization's refusal to produce and distribute a transparency report about its third-party data requests and disclosures. Even though most major and some minor carriers are making these reports available, Bell, considered Canada's largest ISP, continues to fail as a leader in this area.

Table 1. Major Carriers: Star Scores and Improvements Since 2016.

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	
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
Vidéotron	1	0.5	0.5	0.5	0.5		0.5				3.5	1.5
Improvement	1	-0.5	1	0	2	0.5	2	1.5	-0.5	0.5		

Note. An improvement score is not included for Bell MTS. As noted in the sample description, sample updates reflect name changes and mergers/acquisitions.

Table 2 details how some minor carriers also demonstrate increases in data privacy transparency. Distributel and Acanac increased by 5.5 and 6.5 stars, respectively (Acanac previously received zero stars). Again, Distributel is the corporate owner of Acanac. These improvements, along with Storm Internet's increase of three stars are the largest improvements in this group. As noted in Table 3, transit carriers demonstrated no improvement overall (except for Peer 1), and in 8 of 11 cases have fewer stars.

Table 2. Minor Carriers: Star Scores and Improvements Since 2016.

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 Telecom	0.5	0.5		0.5		0.5					2	0
Chatr	0.5	0.5									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 Mobile	1		0.5	0.5	0.5	0.5	0.5				3.5	
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 Internet	1	0.5		0.5	0.5		0.5	0.5			3.5	3
Télébec	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		

Note. Improvement scores not included for Chatr or Freedom Mobile. As mentioned above, sample updates reflect mergers/acquisitions and name changes.

Across the entire sample, an assessment of the individual criteria revealed a few changes. One notable change occurred with scoring on Criterion 5 (personal information definition). Three major carriers, four minor carriers, and four transit carriers received full stars. In 2016, zero major carriers, zero minor carriers, and three transit carriers earned full stars on this criterion. This means that carriers are providing additional details about the types of personal information being collected, as opposed to only referring to generalities. A number of smaller changes in the scoring occurred with regard to Criterion 7 (storage/processing) and Criterion 8 (routing transparency); all majors received a half star or more on 7, whereas three of 10 majors received no stars on this criterion in 2016. For Criterion 8, in 2016, none of the major carriers received a score for this criterion, whereas in the current analysis, three carriers did (Cogeco, Shaw, and TekSavvy). The posting of transparency reports, assessed by Criterion 3, increased from three major carriers in 2016 (Rogers, TekSavvy, and Telus) to five (Rogers, Shaw, TekSavvy, Telus, and Vidéotron).

The assessment across time of the minor carriers revealed similar changes; a number of carriers increased scores for Criteria 5 and 7. The considerable changes in scoring for Criterion 1 suggests that more

minor carriers are providing clearer information about a stated commitment to PIPEDA compliance, and changes to Criterion 6 suggest that more minor carriers are providing references to retention policy.

Table 3. Transit Carriers: Star Scores and Improvements Since 2016.

Carrier	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	Total	Improvement
Allstream											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	
Improvement	0	0	-2	-2.5	-0.5	0	0	-1	0	0		

Note. Improvement scores are not included for Allstream, CenturyLink, or Zayo. Sample updates reflect mergers/acquisitions and name changes.

For the transit carriers, no major improvements were made among the two studies. Again, this is due in part to a lack of data privacy transparency, but also is reflective of the strict approach to study methodology to ensure that the appropriate privacy materials are placed on dedicated sections of carrier websites.

Discussion

This is a third study of the data privacy transparency of ISPs and transit carriers that route Canadian Internet traffic. While some carriers have expanded their data privacy transparency materials and ensured that links and documents are available on dedicated privacy pages, many carriers continue to score poorly.

The modest improvements—acknowledged by the overall increase across the sample from 2.2/10 to 2.6/10 between the 2016 study and the current study—should not be overstated. In most cases, a close inspection of changes to privacy materials revealed minimal details added, with carriers meeting bars set very low for half stars. For example, if, in a single sentence buried in a policy, a carrier was found to mention a country where data storage was taking place, a half star was awarded for Criterion 7. No information or nuance was required about the type or amount of data stored or processed in that country. The type of processing procedures, whether data centers are involved, geo-location of specific data types, city information, or any other information about the data or their location was not required. This lack of detail

is unlikely to support a useful data privacy transparency, contributing little to notice deliverables or digital policy literacy. Similarly, to receive a half star for Criterion 8 (routing transparency), the carrier only had to mention the concept. No explanation of the concept or its implications was required, nor were details about routing procedures, practices, locations, timelines, and so forth. Providing basic details, for the few carriers that did this, is not enough to teach data subjects about the political economic relationships that define routing practices and, as a result, how the Internet operates.

Most Carriers Continue to Provide Little Information About Data Retention

Although some carriers are starting to provide retention information, overall, the companies making slight improvements are disclosing minimal detail about how long they keep data. Acanac and Distributel stand out because they provide a list of data types and the length of time that each is retained. Overall, however, only four majors, six minors, and two transit carriers earned stars in this category. Similar to the data processing scoring, the bar was quite low for a half star. The only requirement was that the carrier provide one mention of a period of time (for example, retaining call logs for 18 months) to receive the half star. Detailed information about the different data types involved, how long each type was kept under different circumstances, justifications for retention policy, and how this approach might contribute to costs for the carrier and for the user were not required. Information about carrier efforts to improve retention practices, future privacy implications, and relationships between retention and secondary or aggregated analyses was not required either. Again, it is essential to keep in mind that providing minimal details does not necessarily help inform data subjects attempting to select the right carrier, or hold that carrier to account. What's more, some carriers disclosed that while they have an internal retention policy, that policy is not made public. For example, Eastlink (2013) stated, "Eastlink has a records retention policy that specifies the length of time that records are maintained" (p. 6). Unfortunately, no details about this policy are available on its privacy pages.

Many Carriers Do Not Provide Details About Personal Information Collected

Many carriers do not provide enough detail about the types of personal information collected. Geo-locations, device identifiers, and other metadata; data from personal video recorders and other set-top boxes; data from home security devices; surveillance data from stores; and various other data types are likely collected by carriers in myriad ways, depending on each carrier's approach. Beyond and related to this are secondary and aggregated analyses unique to each entity asking questions of the data. Indeed, while carriers, including Shaw and Telus, do serve as exemplars (relative to the rest), most carriers provide almost no detail at all, and details about secondary analyses and implications of data collections are essentially absent. It should be noted that among the minor carriers, Bruce Telecom, Chatr, Comwave, Fido, Fongo, VIF Internet, and Xplornet earned zero stars for this criterion.

Transit Carriers Continue to Score Poorly

Digital policy literacy and meaningful online consent could include understanding the role of transit in how the Internet works. Not only are political economic connections between major, minor, and transit carriers unclear, but transit providers continue to fail in their data privacy transparency efforts, demonstrating little interest in helping data subjects learn about the policy, political economic, and infrastructure concerns associated with Internet use. Since the project began in 2013, no transit provider has referenced Canadian privacy law in its privacy materials. This suggests that transit providers have little interest in helping to explain to data subjects in Canada how the Internet works, or that they are involved in the routing of Canadian data. What's more, all transit carriers, aside from AT&T, received fewer stars than the 2.6/10 average. Allstream, Cogent, Hurricane Electric, Level 3, TeliaSonera, and Zayo all received zero stars. The poor scores overall should be especially concerning to those living in Canada, because it further demonstrates how disinterested Internet carriers are in engaging users in the process of Internet governance. Carriers gladly accept data and payment for facilitating Canadian Internet communications; why are they unable to reciprocate and demonstrate leadership in terms of helping to educate and engage users? Keep in mind that ISP-transit relationships are directly responsible for boomerang routing realities, which subject those living in Canada to international routing of domestic Internet traffic at least 22%–25% of the time (Clement & Obar, 2015; Obar & Clement, 2013).

Overall, Carriers Continue to Demonstrate a Lack of Leadership

Carriers often identify themselves as Canada's "best" or "biggest" Internet provider. Rogers describes its 5G network as "the largest in Canada" (Rogers, 2021), Telus claims to have the "largest and fastest network" (Telus, 2021), and Distributel suggests that it is "one of Canada's leading independent Internet service providers" (Distributel, 2021, para. 4). While carriers promote themselves in terms of size and speed, being privacy-forward or a public trustee in the big data context seems to be of little interest in terms of public presence.

The lack of leadership is most notable when assessing Bell Canada, self-described as "Canada's largest communications company" (BCE, 2021). Since the first study in 2013, Bell's score has only increased 0.5 stars. Furthermore, Bell is the only major carrier to score lower than the sample average 2.6/10 stars. To help clarify this poor performance, it should be added that the average score of the other major carriers is 4.9/10, and for the minor carriers 2.9/10. Bell's score is 2.5/10, earning zero stars on criteria emphasizing "a public commitment to inform users of all third-party data requests," "transparency about frequency of third-party (data) requests and disclosures," "the normal retention periods for personal information," "transparency about where personal information is routed," "(Transparency about) domestic Canadian routing when possible," and "open advocacy for user privacy rights."

Indeed, as governments and privacy advocates look for leadership in the privacy space, ISPs and transit carriers seem uninterested in an open, honest, and useful data privacy transparency. Furthermore, any semblance of a public trustee mandate, historically associated with access to the radio spectrum and common carriage (Regan, 2017), is almost completely absent.

Meaningful transparency suggests not only that relevant information should be provided to individuals but also that the information should allow for oversight and control (Ananny & Crawford, 2018; Suzor et al., 2019). Commissioner Daniel Therrien of the Office of the Privacy Commissioner of Canada is clear about one change that is needed to move individuals closer to meaningful online consent: "(Individuals require) better information to empower them to exercise individual control and personal autonomy. . . . Individuals must be at the centre of privacy protection" (OPC, 2017, "Commissioner's Message," para. 3). More information relevant to protecting online privacy is needed, but also more useful information. The intention is that the criteria assessed by this study begin to emphasize the types of information that might be useful to data subjects. It is important to also emphasize that the debate about data privacy transparency is occurring in a context in which individuals are feeling fatigued and resigned in terms of online privacy possibilities (Choi, Park, & Jung, 2018; Draper & Turow, 2019). Therefore, the information and interfaces for communicating that information must also be usable—an area that should continue to be the subject of further research. Far more needs to be done to ensure that meaningful transparency contributes to meaningful online consent, such that users better understand and approve of the digital experience and implications they connect to every day.

References

- Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3), 973–989. doi:10.1177/1461444816676645
- Austin, L. M. (2016). Technological tattletales and constitutional black holes: Communications intermediaries and constitutional constraints. *Theoretical Inquiries in Law*, 17(2), 451–485. doi:10.1515/til-2016-0017
- Ball, C. (2009). What is transparency? *Public Integrity*, 11(4), 293–308. doi:10.2753/PIN1099-9922110400
- BCE. (2021). *BCE overview*. Retrieved from <https://www.bce.ca/about-bce/bce-overview>
- Bell. (2017). *Bell privacy policy*. Retrieved from [https://web.archive.org/web/20170626134914/http://support.bell.ca/_web/guides/Common/Legal/bcfip\(en\).pdf](https://web.archive.org/web/20170626134914/http://support.bell.ca/_web/guides/Common/Legal/bcfip(en).pdf)
- Calo, R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, 87(3), 1027–1072.
- Cate, F. H. (2006). *The failure of fair information practice principles: Consumer protection in the age of the information economy*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81(April), 42–51. doi:10.1016/j.chb.2017.12.001

Clement, A. (2013, June). IXmaps—Tracking your personal data through the NSA’s warrantless wiretapping sites. In *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmented Reality in Everyday Life* (pp. 216–223). Toronto, Canada: IEEE. doi:10.1109/ISTAS.2013.6613122

Clement, A., & Obar, J. A. (2014). *Keeping Internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian Internet service providers*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2491847

Clement, A., & Obar, J. A. (2015). Canadian Internet “boomerang” traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In M. Geist (Ed.), *Law, privacy and surveillance in Canada in the post-Snowden era* (pp. 13–44). Ottawa, Canada: University of Ottawa Press.

Clement, A., & Obar, J. A. (2016). Keeping Internet users in the know or in the dark: An analysis of the data privacy transparency of Canadian Internet carriers. *Journal of Information Policy*, 6(1), 294–331. doi:10.5325/jinfopoli.6.2016.0294

Distributel. (2021). *Who we are*. Retrieved from <https://www.distributel.ca/about-distributel/who-we-are/>

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 1824–1839. doi:10.1177/1461444819833331

Eastlink. (2013). *Code of fair information practices*. Retrieved from https://www.eastlink.ca/Portals/0/About/Code_of_Fair_Information_Practices-Eastlink.pdf

Electronic Frontier Foundation. (2011). *When the government comes knocking, who has your back?* Retrieved from <https://www.eff.org/who-has-your-back-2011>

Federal Trade Commission. (1998). *Privacy online: A report to Congress*. Retrieved from <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>

Freedom of Information and Protection of Privacy Act. (1990–1991). SS 1990-91, c F-22.01. Retrieved from <https://oipc.sk.ca/legislation-main/foip/>

Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L. F., . . . Schaub, F. (2020, April). “It’s a scavenger hunt”: Usability of websites’ opt-out and data deletion choices. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1–12). New York, NY: Association for Computing Machinery. doi:10.1145/3313831.3376511

IXmaps. (n.d.). *Map*. Retrieved from <https://ixmaps.ca/map.php>

Kennedy, H., & Moss, G. (2015). Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society*, 2(2), 1–11. doi:10.1177/2053951715611145

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543–568.

Marwick, A. E., & boyd, d. (2018). Understanding privacy at the margins: Introduction. *International Journal of Communication*, 12, 1157–1165.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4), 32–48.

Obar, J. A. (2015). Big data and *The Phantom Public*: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society*, 2(2), 1–16. doi:10.1177/2053951715608876

Obar, J. A. (2016). Closing the technocratic divide? Activist intermediaries, digital form letters, and public involvement in FCC policy making. *International Journal of Communication*, 10, 5865–5888.

Obar, J. A. (2019). Searching for data privacy self-management: Individual data control and Canada's digital strategy. *Canadian Journal of Communication*, 44(2), 35–41. doi:10.22230/cjc.2019v44n2a3503

Obar, J. A., & Clement, A. (2013, June). 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, Canada.

Obar, J. A., & Oeldorf-Hirsch, A. (forthcoming). *Older adults and "the biggest lie on the Internet": From ignoring social media policies to the privacy paradox*. *International Journal of Communication*.

Oeldorf-Hirsch, A., & Obar, J. A. (2019, July). Overwhelming, important, irrelevant: Terms of service and privacy policy reading among older adults. In *Proceedings of the 10th International Conference on Social Media and Society* (pp. 166–173). New York, NY: Association for Computing Machinery. doi:10.1145/3328529.3328557

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*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

- 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*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/
- Office of the Privacy Commissioner of Canada. (2018). *Guidelines for obtaining meaningful consent*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
- Organisation for Economic Co-operation and Development. (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. Retrieved from <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>
- Parsons, C. (2019). The (in) effectiveness of voluntarily produced transparency reports. *Business & Society*, 58(1), 103–131. doi:10.1177/0007650317717957
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.
- Personal Information Protection and Electronic Documents Act. (2000). S.C. 2000, c. 5. Retrieved from <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html>
- Regan, P. M. (2017). Reviving the public trustee concept and applying it to information privacy policy. *Maryland Law Review*, 76(4), 1025–1043.
- Reidenberg, J. R., Breaux, T., Cranor, L., French, B., Grannis, A., Graves, J. T., . . . Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30(1), 39–68.
- Rogers. (2021). *Wireless*. Retrieved from <https://www.rogers.com/5g>
- Schaub, F., Balebako, R., & Cranor, L. F. (2017). Designing effective privacy notices and controls. *IEEE Internet Computing*, 21(3), 70–77. doi:10.1109/MIC.2017.75
- Schudson, M. (2015). *The rise of the right to know: Politics and the culture of transparency, 1945–1975*. Cambridge, MA: Harvard University Press.
- Shade, L. R., & Shepherd, T. (2013). Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday*, 18(12). doi:10.5210/fm.v18i12.4807
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903.

Suzor, N. P., West, S. M., Quodling, A., & York, J. (2019). What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. *International Journal of Communication*, 13, 1526–1543.

Telus. (2021). *Building Canada's largest and fastest network*. Retrieved from <https://www.telus.com/en/social-impact/blog/building-largest-and-fastest-network>

Woolery, L., Budish, R. H., & Bankston, K. (2016). *The transparency reporting toolkit: Best practices for reporting on U.S. government requests for user information*. The Berkman Klein Center for Internet & Society. Retrieved from <https://dash.harvard.edu/handle/1/28552578>