KEEPING INTERNET USERS

IN THE KNOW OR IN THE DARK

Data Privacy Transparency of Canadian Internet Service Providers

Andrew Clement & Jonathan Obar

ANDREW.CLEMENT@UTORONTO.CA · JONATHAN.OBAR@UTORONTO.CA

IXmaps.ca & New Transparency Projects

Faculty of Information, University of Toronto

March 27, 2014

IXmaps

WWW.IXMAPS.CA

ACKNOWLEDGEMENTS

We appreciate the contributions of our research collaborators and assistants at the University of Toronto: Andi Argast, Alex Cybulski, Lauren DiMonte, Antonio Gamba, Colin McCann and Nancy Paterson (OCAD University). We would also like to acknowledge the input of Steve Anderson, Nate Cardozo, Tamir Israel, Christopher Parsons, Christopher Prince and Rainey Reitman.

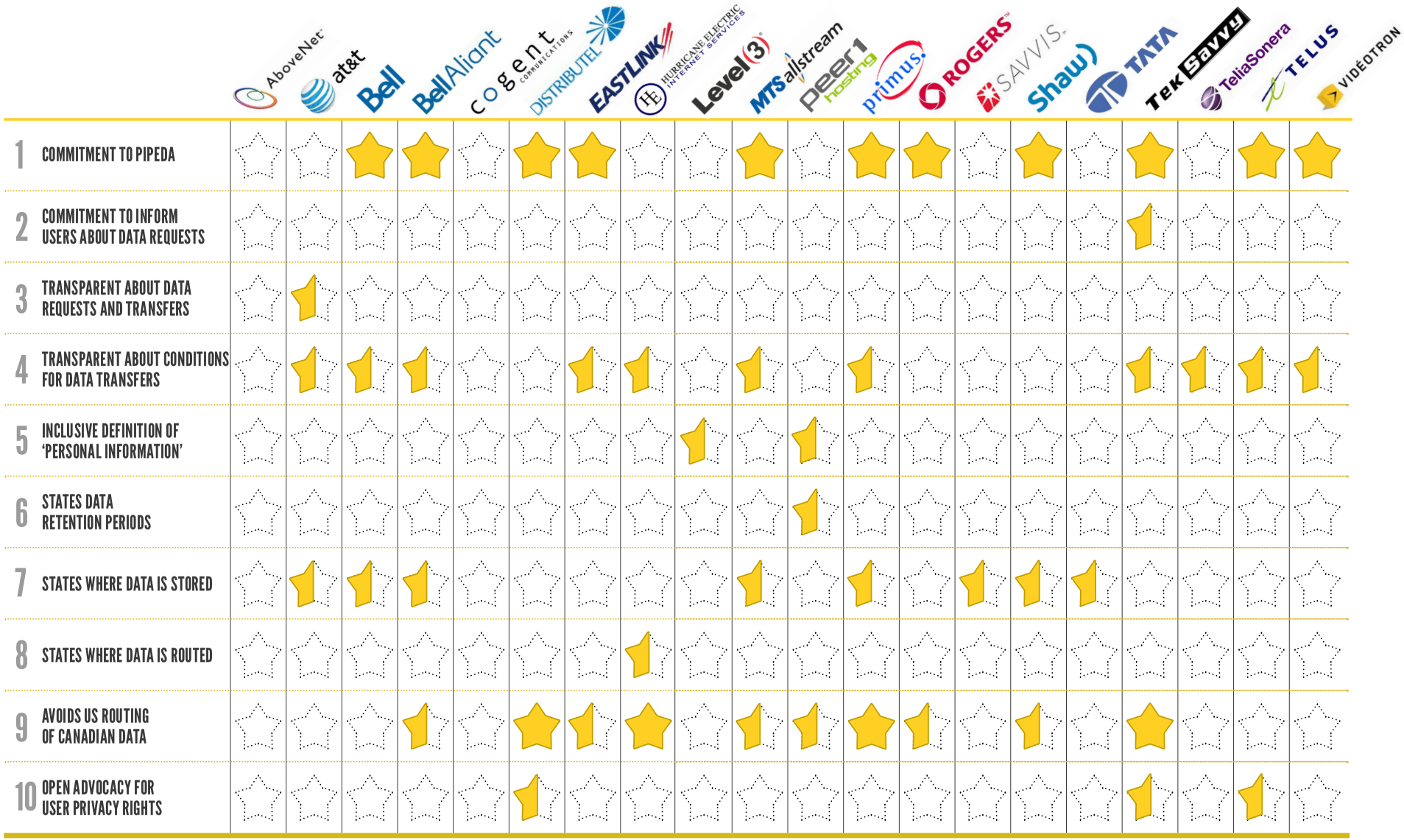
Website and report design assistance: Jennette Weber.

This research was conducted under the auspices of the *IXmaps: Mapping Canadian privacy risks in the internet 'cloud'* project (see WWW.IXMAPS.CA) and the Information Policy Research Program (IPRP) (see WWW.IPRP.ISCHOOL.UTORONTO.CA), with the support of the Office of the Privacy Commissioner of Canada as well as *The New Transparency: Surveillance and Social Sorting* project (see WWW.SSCQUEENS.ORG/PROJECTS/THE-NEW-TRANSPARENCY) funded by the Social Sciences and Humanities Research Council.

The views expressed are of course those of the authors alone.

The report is available at WWW.IXMAPS.CA/TRANSPARENCY.PHP.

The Data Privacy Transparency *of* Canadian Internet Service Providers



EXECUTIVE SUMMARY

In the wake of the Snowden revelations about NSA surveillance, recent calls for greater data privacy recommend that internet service providers (ISPs) be more forthcoming about their handling of our personal information. Responding to this concern as well as in keeping with the transparency, openness and accountability principles fundamental to Canadian privacy law, this report evaluates the data privacy transparency of twenty of the most prominent ISPs (aka carriers) currently serving the Canadian public. We award ISPs up to ten 'stars' based on the public availability of the following information:

1. A public commitment to PIPEDA[1] compliance.
2. A public commitment to inform users about all third party data requests.
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 period for personal information.
7. Transparency about where personal information is stored.
8. Transparency about where personal information is routed.
9. Publicly visible steps to avoid U.S. routing of Canadian data.
10. Open advocacy for user privacy rights (such as in court and/or legislatively).

These criteria are designed to address on-going privacy and civil liberties concerns, especially in light of the controversial expansion of state surveillance of internet activities as well as recent 'lawful access' proposals, notably Bill C-30 and the current Bill C-13.

Stars are awarded based on careful examination of each ISP's corporate website. Assuming that carriers want to make it easy for their customers to find information about corporate practices relating to personal information, and that the on-line privacy policy is the first (and only) place users might look, we focus our attention on these public statements[2].

We selected the 20 ISPs in our sample based on their prevalence among the approximately 6000 internet traceroutes in the IXmaps.ca database (out of 25,000+ in total) that correspond to intra-Canadian routes – i.e. with origin and destination in Canada. The star ratings can be seen in the accompanying Star Table.[3] The Appendix contains the detailed assessments for each carrier.

1. Personal Information Protection and Electronic Documents Act

2. In the case of criterion 9—*Publicly visible steps to avoid U.S. routing of Canadian data*, we also examine the peering arrangements noted on the websites of the two main Canadian public internet exchanges, TorIX and OttIX (Toronto/Ottawa Internet Exchanges) as these are also publicly visible.

3. Star ratings can also be reviewed for particular internet routings and carriers on the Explore page of the IXmaps website (http://ixmaps/explore)

FINDINGS

As the Star Table makes clear, ISPs earn very few stars – 1.5/10 on average. The highest scoring carrier overall is TekSavvy, earning 3.5 stars in aggregate based on full or half stars across five criteria. The large foreign carriers Cogent and AboveNet (Zayo) receive no stars.

Slightly more than half of the ISPs (11 of 20), all operating primarily in Canada, state a commitment to adhere to the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs the handling of personal information in commercial transactions. None of the foreign-based ISPs that carry significant amounts of intra-Canadian traffic indicate any explicit compliance with Canadian privacy law. Foreign carriers expose personal data to US and other jurisdictions, where Canadian data is largely unprotected legally from foreign state surveillance. This is especially concerning because while Canadians can work to influence the activities of a democratically governed Canadian state surveillance apparatus, Canadians' ability to affect the activities of foreign governments is relatively limited.[4]

No Canadian ISP has yet published a transparency report along the lines of AT&T, Verizon, Google, Facebook or Twitter, each of which have begun to report standardized statistics concerning law enforcement access requests.

Policy Recommendations

Without proactive public reporting on the part of ISPs in the key areas identified above, it is very difficult for Canadians to protect their personal privacy online nor hold these important organizations to account. To remedy this situation, we make the following recommendations directed at prime internet privacy actors:

For ISPs/carriers that handle Canadian Internet traffic:

ISPs should to go beyond minimum compliance with Canadian privacy law, and, in the spirit of PIPEDA's *Principle 8 – Openness*, commit proactively to making the information identified by the ten criteria readily available publicly. In particular, they should publish on the privacy sections of their corporate websites:

Recommendation 1: A public commitment to PIPEDA compliance,

Recommendation 2: A public commitment to inform users when personal data has been requested by a third party,

Recommendation 3: Regular, detailed transparency reports that provide information about third party data requests and disclosures,

Recommendation 4: Detailed conditions and procedures for law enforcement and other third parties that submit requests for personal information,

4. It is worth noting that personal information that is kept within Canadian jurisdiction is also subject to state surveillance activities; however, Canadian entities conducting surveillance within Canada are subject to Canadian lawand its Constitution. Should Canadians determine that the Canadian surveillance apparatus is to change, that would possibly affect the level of surveillance on intra-Canadian traffic. The same cannot be said about traffic that passes through the US and other foreign countries as Canadians cannot easily force change in the laws and surveillance practices of foreign countries.

Recommendation 5: A clear indication that metadata and device identifiers are included in the definition of 'personal information',

Recommendation 6: Retention periods and the justification for these, for the various types of personal information handled,

Recommendation 7: Details of whether personal data may be stored or routed outside Canada,

Recommendation 8: How they strive to keep Canadians' data within Canadian legal jurisdiction,

Recommendation 9: How they strive to keep Canadians' data protected against mass Canadian state surveillance,

Recommendation 10: The extent to which they advocate for their subscribers' privacy rights.

For Privacy Commissioners and the Canadian Radio-Television and Telecommunications Commission (CRTC).

Recommendation 11: Regulators should more closely oversee ISPs to ensure their data privacy transparency.

For legislators and politicians.

Recommendation 12: Amend PIPEDA's Principle 8 — Openness to include public transparency.

Recommendation 13: Amend PIPEDA's Principle 9 — Individual Access to require proactive notification

Recommendation for Canadian law enforcement and security agencies

Recommendation 14: Canadian law enforcement and security agencies should proactively publish statistics about requests for personal information they make to ISPs.

These various measures advancing data privacy transparency will contribute to ensuring that ISPs and third party data requestors are accountable to the Canadian public for their data management practices. Those actors adopting strong transparency measures will demonstrate leadership in the global battle for data privacy protections, and help bring state surveillance under more democratic control.

TABLE OF CONTENTS

Star Table **3**

Executive Summary **4**
Findings 5
Policy Recommendations 5

Background **9**
Transparency and the "Openness Principle" 9
Why Assess Transparency? 10

Assessing Data Privacy Transparency **11**
Selecting ISPs 11
Awarding Stars to ISPs 12
Evaluation Criteria **12**
1: A public commitment to PIPEDA compliance 13
2: public commitment to inform users about all third party data requests 13
3: Transparency about frequency of third party data requests and disclosures . 14
4: Transparency about conditions for third party data disclosures 14
5: An explicitly inclusive definition of 'personal information' 15
6: The normal retention period for personal information 15
7: Transparency about where personal information is stored 16
8: Transparency about where personal information is routed 16
9: Publicly visible steps to avoid U.S. routing of Canadian data 16
10: Current political position in terms of the 'fight' for user privacy rights 17

Findings **18**
ISPs all score poorly 18
Smaller, independent Canadian carriers score better than larger incumbents . . 18
Canadian carriers score better than foreign ones 18
TekSavvy scores highest 18
PIPEDA compliance is minimal and partial at best 18
No proactive transparency reporting 18
Routing transparency is almost entirely absent 19
ISPs rely heavily on implied consent 19

Policy Recommendations **19**
1: A public commitment to PIPEDA compliance 19
2: A public commitment to inform users when personal data has been requested by a third party 20
3: Regular detailed transparency reporting that provides information about third party data requests and disclosures 20

4: Detailed conditions and procedures for law enforcement and other third parties that submit requests for personal information 20
5: A clear indication that metadata and device identifiers are included in the definition of 'personal information' 20
6: Retention periods and the justification for these, for the various types of personal information handled 20
7: Details of whether personal data may be stored or routed outside Canada . . . 21
8: How they strive to keep Canadians' data within Canadian legal jurisdiction 21
9: How they strive to keep Canadians' data protected against mass Canadian state surveillance 21
10: The extent to which they advocate for their subscribers' privacy rights. 21
11: Regulators should more closely oversee ISPs to ensure their data privacy transparency 22
12: Amend PIPEDA's Principle 8 — Openness to include public transparency. . . 22
13: Amend PIPEDA's Principle 9 — Individual Access to require proactive notification 22
14: Canadian law enforcement and security agencies should proactively publish statistics about requests for personal information they make to ISPs 22

Appendix: ISP Profiles and Evaluations 23
AboveNet Communications (ZAYO) 24
American Telephone and Telegraph (AT&T) 25
Bell Canada 27
Bell Aliant 29
Cogent Communications 31
Distributel Communications 32
Eastlink 34
Hurricane Electric Internet Services 36
Level 3 Communications 38
MTS Allstream 40
Peer 1 Hosting. 42
Primus Telecommunications (Canada). 44
Rogers Communications 46
Savvis Communications (CenturyLink) 47
Shaw Communications 49
TATA Communications 51
TekSavvy Solutions 53
TeliaSonera 56
TELUS 58
Vidéotron 60

About the Report 61

KEEPING INTERNET USERS IN THE KNOW OR IN THE DARK

A Report on the Data Privacy Transparency of Canadian Internet Service Providers

BACKGROUND

In Canada we entrust the enormous quantities of personal data produced by our online activities to a select group of internet service providers (ISPs). These ISPs, also referred to as carriers or telecommunication service providers,[5] carry, transmit, and route our data back and forth over the internet between our personal devices (laptops, smartphones, etc.) and email servers, websites, social networking sites, and other services. Long-standing privacy concerns about how this personal information may be monitored or surveilled have been heightened by the on-going Snowden revelations. We now have strong evidence that state surveillance agencies, such as the US National Security Agency (NSA) and Communications Security Establishment Canada (CSEC), have secretly gained the cooperation of telecommunications companies to access, store and analyse our personal data.

Knowing more about what ISPs do with our data has become urgent. When a company or law enforcement agency demands access, do ISPs comply? Do they inform us about it? Do ISPs route or even store our data beyond Canadian legal protection? When it comes to data privacy protection, do ISPs keep us in the know or in the dark?

Transparency and the "Openness Principle"

This report evaluates the data privacy transparency of the most prominent ISPs serving the Canadian public. The call for greater privacy transparency in Canada, as presented by this report, draws from a long history of privacy principles adopted by international bodies and nation states around the world, dating back at least to the OECD's Privacy Principles of 1980. In particular, the OECD's "Openness Principle" which states,

> *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.*[6]

Since the OECD's principles were published more than 40 years ago, other calls for data privacy transparency have built on their fair information practice principles, including the EU's 1995 Data Protection Directive[7] and the White House's 2012 Consumer Privacy Bill of

5. The focus of this report is on those internet service providers that carry Canadian data across telecommunications networks, rather than store or process it, so we'll use the terms 'ISP' and 'carrier' interchangeably.

6. http://oecdprivacy.org/

7. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Rights.[8] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which since 2001 has regulated privacy in commercial transactions, fits squarely in this transparency tradition. Its Openness Principle (PIPEDA Principle 8) states,

> *An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*[9]

Why Assess Transparency?

While the general principle of transparency or openness is by now very well established, its actual practice falls far behind the ideal in many areas of commercial consumer/corporate relations. Canadian privacy legislation as implemented strongly favours a (largely illusory) informed consumer choice model over a public accountability model of privacy protection. As the Openness Principle of PIPEDA indicates, the burden is on individuals to ask specific questions about the handling of their own information. It requires a concerted effort to find out just what is being done with one's own information, putting this beyond the ability of all but the most determined individuals. It then requires further exertion to share what's learned more widely; not to mention the need for repeated inquiry to ensure continued protections.

This report seeks to overcome the systemic barriers to data privacy transparency in the case of the telecommunication service providers. This currently is an area of special concern given the growing evidence of mass state surveillance. Adopting a public accountability approach we examine the privacy materials made public by the twenty most prominent internet carriers serving the Canadian public. We highlight those that not only claim to meet the letter of their legal responsibilities under PIPEDA, but in the spirit of Principle 8 – Openness, go beyond minimum compliance requirements by making important aspects of their handling of personal data publicly transparent. In doing so, we aim to help Canadians understand better the privacy risks of using the internet and which ISPs are more transparent about their privacy practices.

While this is the first Canadian study of ISP data privacy transparency, it is inspired by and contributes to the growing number of similar efforts championing data privacy transparency around the world. These include: Transparency reports from AT&T,[10] Verizon[11], Google,[12]

8. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
9. http://www.priv.gc.ca/leg_c/p_principle_e.asp
10. http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
11. http://transparency.verizon.com/
12. http://www.google.com/transparencyreport/

Microsoft,[13] Twitter,[14] Dropbox,[15] Linkedin,[16] Facebook,[17] and others; the Electronic Frontier Foundation (EFF)'s 'Who Has Your Back' reports;[18] and the 'Ranking Digital Rights' Project (led by Rebecca McKinnon (New America Foundation) and University of Pennsylvania).[19] Our study also complements the work of Dr. Christopher Parsons at the University of Toronto's Citizens Lab.[20] While Parsons uses an in-depth questionnaire approach, like the EFF we highlight and compare what ISPs report publicly.

By drawing attention to important but too often obscure personal data handling practices of ISPs and recognizing those carriers that are relatively open, we hope to encourage carriers to be more proactively transparent and take stronger public stands for user privacy. To be clear, we are not rating the actual privacy protections ISPs offer – that would require a different study – but assessing a vital ingredient of data privacy – transparency. We don't seek to rank ISPs as much as to cheer on those providers that are especially transparent about how they handle our personal information.

ASSESSING DATA PRIVACY TRANSPARENCY

We modeled this report most directly on the EFF's "Who's Got Your Back" annual report. Ours takes an explicitly Canadian orientation, focusing specifically on carriers, rather than service providers more generally, while broadening the range of criteria to highlight those that are particularly relevant to contemporary privacy concerns in Canada.

Selecting ISPs

We chose 20 ISPs for this first Canadian study based not just on their familiarity to Canadians, but specifically on the degree to which they actually carry intra-Canadian internet traffic. We assessed this by drawing on the database of traceroutes that the IXmaps.ca research project has accumulated by crowdsourcing methods since 2009. Currently the database contains over 25,000 traceroutes, of which ~6,000 we categorize as intra-Canadian, i.e. they originate and terminate in Canada, whether or not they are routed entirely within Canada (many are routed through the US, in what we refer to as 'boomerang' routing'). We examined these 6000 traceroutes for the ISPs that carried traffic beyond the immediate origination and destination. While we make no claim that the database is representative of all Canadian internet traffic, we regard our sample as large and diverse enough that nearly all

13. https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
14. https://transparency.twitter.com/
15. https://www.dropbox.com/transparency
16. http://help.linkedin.com/app/answers/detail/a_id/41878
17. https://www.facebook.com/about/government_requests
18. https://www.eff.org/who-has-your-back-2013
19. http://rankingdigitalrights.org/
20. Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/ http://www.ottawacitizen.com/technology/Internet+firms+play+they+share+info+with+police+government/9586411/story.html

carriers of significance will show up in it.[21]

The resulting selection includes the major Canadian telecom carriers (Bell, Bell Aliant, MTS Allstream, Rogers, Shaw, Telus and Videotron), as well as several of their smaller Canadian competitors (Distributel, Eastlink, Primus Canada[22] and Teksavvy). But importantly it includes those ISPs that do not have a local, retail presence in Canada but serve as network operators, handling traffic behind the scenes, in the 'backbone' or 'core' of the internet. These include a Canadian networking provider (Peer-1), large well known US carriers (AT&T), and large international internet backbone operators (AboveNet, Cogent, Hurricane, Level-3, Savvis, Tata and TeliaSonera). These latter foreign carriers are significant, not only because they are largely invisible to Canadian consumers, but also because they operate under foreign jurisdictions and usually route intra-Canadian data through the US and outside Canadian legal and constitutional protection.

Awarding Stars to ISPs

Carriers earn 'stars' for each of the following 10 criteria. In what follows, we provide a brief rationale and description for each criterion, as well as illustrative examples from our study. Where no ISP in our sample earns a full star, we offer an exemplar from the EFF's report.

We award stars based on readily available evidence presented on the ISP's corporate website. On the premise that carriers would want to make it easy for their customers to find relevant information about corporate practices around personal information, and that the on-line privacy policy is where users would look first (and likely not look further), we confined our attention to these public statements. All but one carrier (Cogent) had such an on-line privacy policy.[23]

A further advantage of this approach is that individual internet users can check that our results are correct, or apply these criteria to additional carriers. We look forward to receiving feedback and will update the report accordingly.

We provided all ISPs evaluated with the opportunity to respond to a preliminary version of this report and our initial transparency assessment. We took their comments into consideration for the current analysis and re-checked their websites to see if they had updated their public statements in light of our assessment. In one case, MTS Allstream, the website did subsequently provide more public disclosure and we awarded a higher score as a result. We last verified all ratings at the end of 2013.

Evaluation Criteria

Data privacy transparency is a broad and evolving concept, with an (over-)abundance of possible criteria upon which to assess it. In our case we began this work in early 2013 with

21. A possible exception to this is Cogeco, which is a significant Canadian ISP, but did not appear prominently in our database. We plan to include Cogeco in the next edition of this Report.

22. Primus Canada operates exclusively within Canada, but is owned by a U.S. parent, Primus Telecommunications.

23. The sole exception to the exclusive focus on corporate privacy and related statements is in the case of Criterion #9, as discussed below.

the criteria EFF used in its 2012 Who's Got Your Back report (e.g. informing users of 3rd party requests, corporate transparency reporting, fighting for user privacy in the courts and legislature). We supplemented these with criteria directly related to current Canadian controversies around personal privacy and civil liberties – the defeated Bill C-30 'lawful access' proposal[24] and concerns about the US 'boomerang' routing of Canadian domestic internet traffic through the US in particular (e.g. definition of personal information, data retention periods, locational jurisdiction of data storage and routing). Their relevance has been subsequently heightened in light of the Snowden revelations of the extraordinary expansion of mass state surveillance of internet activities as well as the re-incarnation of lawful access legislation in the form of Bill C-13 — the Protecting Canadians from Online Crime Act.[25].

The 10 criteria are as follows:

1) A public commitment to PIPEDA compliance

All enterprises in Canada that collect personal information as part of their commercial activities must comply with the Personal Information Protection and Electronic Documents Act (PIPEDA). But do they tell us this? It should be easy.

The ISP earns a star if it explicitly indicates compliance with PIPEDA or other comparable Canadian privacy legislation. We reviewed the Privacy sections of ISP websites for direct quotations from PIPEDA and/or a statement of commitment referring to the legislation. An example that earns a full star: Rogers notes the following in their privacy statement:

> *Rogers' privacy practices are in accordance with all federal and provincial laws and regulations. We are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA) and where applicable with the privacy rules established by the Canadian Radio-television and Telecommunications Commission (CRTC).*

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

Under PIPEDA, Principle 9 – Individual Access, individuals have a right to be informed when the government or other third parties request disclosure of their personal information.

Does the ISP explicitly indicate that it informs users when a third party has sought their personal data, unless prohibited by law? An example can be found in Teksavvy's 'Copyright FAQ':

> *How will I know if TekSavvy has received a request for my personal information? TekSavvy will notify you by email and provide as much information it has available about the legal proceeding under which the request is made. […] How will I know if TekSavvy has disclosed my personal information? TekSavvy will notify affected customers if we receive a court order to disclose their personal information.*

This earns a half star because the statement appears to apply only in the case of alleged copyright infringement, and not more generally.

---

24. Bill C-30 — the Protecting Children from Internet Predators Act

25. **http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6311444&File=27#1**

An example that would earn a full star (though they are not a carrier serving Canadians) can be found in Twitter's 2012 transparency report:

> *We notify affected users of requests for their account information unless we're prohibited by law. More information about user notice is available in our Guidelines for Law Enforcement.*

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

Many companies have begun proactively to publish Transparency Reports, summarizing the various kinds of requests for personal data from third parties and how they have responded.

Does the ISP report statistics about the number of requests for data from third parties such as government, law-enforcement, commercial and non-commercial entities, whether it has complied with these requests, how many accounts were covered by these requests and subsequent disclosures? We searched ISP websites for transparency reports noting this information. Examples that would earn full or half-stars: AT&T, Verizon, Google, Twitter, Facebook and Microsoft have each recently begun releasing reports detailing similar requests by law enforcement agencies.

4) Transparency about conditions for third party data disclosures

Companies do have the authority under PIPEDA to provide voluntarily personal information about their customers to third parties under specific circumstances, but it is typically hard to tell what these conditions are and what criteria third party requestors need to meet. This has been a contentious issue in the lawful access debate, since telecommunications companies are routinely providing law enforcement and security agencies with access to personal data without warrants.[26]

Does the ISP provide explicit details clarifying the specific conditions for all third party disclosures, especially instances where informed consent is not given, or where there are requirements that compel disclosures. The clearest of these is MTS Allstream's statement:

> *The Company may also collect, use and disclose personal information without knowledge or consent if: a) seeking the consent of the individual might defeat the purpose of collecting the information, such as in the investigation of a breach of an agreement or a contravention of a federal or provincial law; b) there is an emergency where the life, health or security of an individual is threatened; or c) disclosure is to a lawyer representing the Company, to collect a debt, to comply with a subpoena, warrant or other court order, or otherwise required or permitted by law.*

This statement earned a half-star because it was not explicit about what documentation is required of law enforcement when requesting access to personal information.

An example that would receive a full star (not a Canadian ISP) can be found in Google's recent transparency report. In the "Legal Process" section, Google describes in detail what is required for the U.S. government to request data. Here is an excerpt:

---

26. Paul McLeod, "Ottawa has been spying on you: Telecom firms handing over data without warrants," Chronicle Herald, March 26, 2014. **http://thechronicleherald.ca/novascotia/1195828-ottawa-has-been-spying-on-you**

Does a law enforcement agency in the U.S. have to use legal process to compel Google to provide user data or will a phone call be enough?

The government needs legal process—such as a subpoena, court order or search warrant to force Google to disclose user information. Exceptions can be made in certain emergency cases, though even then the government can't force Google to disclose.

5) An explicitly inclusive definition of 'personal information'

'Personal information,' or 'information about an identifiable individual', is legally protected in Canada, but there is considerable controversy of what it consists of. Unique, persistent, device identifiers, such as IP addresses, MAC addresses, IMSEI numbers and the like are often closely associated with identifiable individuals and routinely used in tracking people. 'Meta-data', or data derived from a communication more generally, can also be highly sensitive and revealing about a person's activities, the people they associate with, their beliefs, health conditions and much more.

Does the ISP state that it treats IP addresses and other unique device identifiers, as well as meta-data (e.g. who communicated with whom, when, where, etc.) where appropriate, as personal information? Though they are not a Canadian ISP, Twitter provides an example that would have received a full star. Their privacy statement provides a detailed description of the various forms of personal information that Twitter collects; including (but not limited to): registration information, account settings, tweets, location information, links, cookies, log data, widget data and other data collected by third parties like IP addresses.

A second example takes a good step in the right direction but received a half-star because it does not explicitly include meta-data: Distributel provides the following definition of personal information:

P.I.P.E.D.A. defines personal information as "information about an identifiable individual". Simply said, any information that is not readily available to the public is protected under the act, for example: credit records, ethnicity, passwords, income etc."

Since unique device identifiers and meta-data are 'not readily available to the public', these are included implicitly in this definition.

6) The normal retention period for personal information

How long a company keeps personal information is a privacy issue because the longer it is kept, the longer it is potentially subject to disclosure or mis-use.

Does the ISP specify the number of days that data is normally retained? Data-specific retention period variations should be noted. In Canada, ISPs typically include statements like this:

"We keep your Personal Information as long as we need for business, tax or legal purposes."

While meeting minimum legal requirements, it is too ambiguous to be useful to customers.

An example that would receive a full star (not a Canadian ISP): Sonic.net's "Legal Process Policy" statement notes its retention policies for the following types of information:

IP logs: 0-14 days; call records 18 months; preservation requests: 90 days; other records: variable.

A second example that receives a half-star because only log files are noted: TekSavvy's website states:

> *"TekSavvy currently stores log files for 90 days. In cases where legal proceedings are initiated by a holder of copyrights, we may be required to retain the logs until the litigation is concluded."*

7) Transparency about where personal information is stored

Where one's data is stored is a privacy issue because it determines which legal jurisdiction it is covered by. Canadians' personal data stored outside Canada generally enjoys lower legal protection than when at home. In the US in particular, it is subject to the Patriot Act and the FISA Amendments Act and treated as foreign, meaning no effective legal safeguards against NSA surveillance.

Does the ISP indicate the relevant geographic location(s) for storage of personal data? An example that receives a half-star (because of ambiguity): Bell's privacy policy describes the possibility of foreign storage of Canadian data:

> *In some cases, personal information collected by the Bell companies may be stored or processed outside of Canada to provide you with the service or to support Bell operations, and may therefore be subject to the legal jurisdiction of these countries.*

8) Transparency about where personal information is routed

As with data storage mentioned above, data routing also affects legal privacy protection, even if the time spent in the foreign jurisdictions is just a fraction of a second. In particular, as IXmaps research has shown, much of domestic Canadian domestic internet traffic (~25%) follows "boomerang routing" - communication that starts in Canada and ends in Canada, but which passes through the US, where it almost certainly subject to NSA surveillance.

Does the ISP indicate the relevant geographic location(s) for routing of personal data? An example that receives a half-star as it does not clarify for Canadians that their data may be routed through the United States: Hurricane's 'About' page notes that they have

> *"no less than four redundant paths crossing North America, two separate paths between the U.S. and Europe, and rings in Europe and Asia."*

Hurricane's 'Network Information' link brings users to a detailed network map. They also provide additional peering information, and a network looking glass.

9) Publicly visible steps to avoid U.S. routing of Canadian data

Given the additional privacy and surveillance risks facing Canadians' personal data when traveling outside Canada, there are good privacy reasons for routing this data within Canada.[27] One of the best ways for ISPs to ensure all-Canadian routing is if they were to exchange traffic (peer) openly at Canadian public internet exchanges points (IXPs), such as TorIX (Toronto Internet Exchange) and OttIX (Ottawa internet exchange).

27. There are also good economic reasons for keeping Canadian data within Canada, as the Canadian Internet Registration Authority (CIRA) makes clear in its report with the Packet Clearing House: Toward Efficiencies in Canadian Internet Traffic Exchange, by Bill Woodcock & Benjamin Edelman, Sept. 2012.

Does the ISP take clear steps to ensuring that personal data transmissions are routed through Canadian internet exchange points unless non-Canadian routing is absolutely necessary? In addition to ISP sites, we reviewed the TorIX and OttIX websites. 'Conditional' peering arrangements receive half-stars, arrangements without noted conditions receive full stars. For example, as noted in the Figure 1 below captured from the TorIX site, Peer 1, Rogers and Shaw have conditional arrangements, and Primus peers without conditions.

Peer1 Hosting	13768	206.108.34.159	2001:0504:001A::34:159	conditional
Persona Inc.	23184	206.108.34.20	2001:0504:001A::34:20	accepting
PostMedia Network Inc.	18588	206.108.34.191	2001:504:1A::34:191	accepting
Primus Telecommunications CA Inc.	6407	206.108.34.22		accepting
Priority Colo Inc.	30176	206.108.34.41	2001:0504:001A::34:41	accepting
Prodosec Inc.	53441	206.108.34.150	2001:0504:001A::34:150	accepting
PurePages Inc.	53424	206.108.34.154	2001:0504:001A::34:154	accepting
Q9 Networks Inc.	12188	206.108.34.13	2001:0504:001A::34:13	conditional
Quadro Communications Co-operative Inc.	25914	206.108.34.176	2001:0504:001A::34:176	accepting
RackForce Networks Inc.	19875	206.108.34.165		accepting
Radiant Communications Corp.	21724	206.108.34.102	2001:0504:001A::34:102	conditional
Ravand Cybertech Inc	12212	206.108.34.222		accepting
RISQ	376	206.108.34.163	2001:0504:001A::34:163	conditional
Rogers Communications Inc.	812	206.108.34.29	2001:0504:001A::34:29	conditional
RU Networks	18997	206.108.34.215		connecting
Ruralwave	46525	206.108.34.201	2001:504:1A::34:201	accepting
Saskatchewan Telecommunications	803	206.108.34.96		conditional
Seaside Communications	47027	206.108.34.134	2001:0504:001A::34:134	accepting
Selectcom Telecom	40224	206.108.34.213		accepting
Sentex Communications Corporation	11647	206.108.34.18	2001:0504:001A::34:18	accepting
Server North Inc.	32881	206.108.34.95	2001:0504:001A::34:95	accepting
Shaw Communications Inc.	6327	206.108.34.12		conditional

Figure 1 Screenshot of Peering Data Noted on the Toronto Internet Exchange (TorIX) Site

10) Current political position in terms of the 'fight' for user privacy rights

Given the important role ISPs play in handling personal information, customers interested in protecting their data will be interested to know where their ISP stands on privacy issues, especially as these come up in court cases or in the proposals for 'awful access'. Canadians showed in the 2012 debate over the proposed Bill C-30 that they were strongly opposed greater government access to this data, but their ISPs were quietly supportive.

Does the ISP make clear its recent (since 2010) legal and/or legislative positions regarding user privacy rights. This demonstration could include reference to political position, legal cases, legislative processes, and ties to advocacy. An example that receives a half-star is TekSavvy, which has a section of its site devoted to the Voltage Pictures v. John and Jane Doe case, in which it gives guidance to its subscribers on how they might handle contact with Voltage Pictures.

Review of the popular press and personal communication with ISPs also revealed that some ISPs have been involved in court cases. To demonstrate support for these efforts, even though mentions were generally absent from their websites, half-stars were awarded for all ISPs that since 2010 have defended user rights in court.

FINDINGS

ISPs all score poorly

As noted in the Star Table, while we able to award at least one half star in each of the criteria, we were only able to award very few stars overall (31.5 out of a possible 200). For individual ISPs, this means an average of 1.5 out of a maximum of 10. The highest ISP score is 3.5 stars (Teksavvy), another earned 3 stars (Primus), followed by three each earning 2.5 stars (Bell Aliant, Distributel and MTS Allstream.

Smaller, independent Canadian carriers score better than larger incumbents

The large incumbent Canadian ISPs (Bell, Bell Aliant, MTS Allstream, Rogers, Shaw, Telus, Videotron) averaged 2 stars, while their smaller independent competitors scored 2.75. All but one of these, Eastlink, scored at least as well as the highest scoring incumbent. An important contributor to this discrepancy is that these small carriers generally peer openly at Canadian public internet exchange points, whereas none of their larger competitors do.

Canadian carriers score better than foreign ones

The highest scoring non-Canadian carrier, Primus Canada, received 3 stars. It was the only foreign carrier to indicate compliance with PIPEDA (Criterion #1). Cogent and AboveNet received no stars. In a counter-privacy form of transparency, Cogent makes clear to customers that they should not expect protection for their personal data:

> *Cogent makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Cogent technology, and makes no guarantee that any other entity or group of users will be included or excluded from Cogent's network.*

TekSavvy scores highest

In addition to receiving more stars in aggregate than any other carrier (3.5), TekSavvy stands out from the others by earning stars in more criteria (5) than any other and is the only ISP to receive recognition (half star) for Criteria 2: Public commitment to inform users about third party data requests. TekSavvy also distinguishes itself as the only ISP to discuss its stance on user privacy rights on its website by informing customers how they treat third party requests and the presentation of court documents. This is chiefly in relation to the Voltage Pictures filesharing suit. ISP subscribers shouldn't have to wait until court cases arise to be told basic information about how their carriers treat third party requests and fight for their rights.

PIPEDA compliance is minimal and partial at best

Of all the criteria, we awarded the highest number of stars (11/20) for Criterion #1: A public commitment to PIPEDA compliance. Exclusively, these are ISPs operating mainly in Canada, and of these very few went significantly beyond stating their compliance. Retention periods and handling of third party requests are left vague. As noted, Primus was the only foreign owned carrier to indicate PIPEDA compliance, even though the others have major Canadian operations (Cogent, Hurricane, Tata). This finding should of considerable concern to Canadians because many Canadian ISPs that do claim PIPEDA compliance often hand traffic to these non-US carriers that seemingly ignore Canadian privacy law.

No proactive transparency reporting

No carrier providing internet services directly to Canadians has yet followed the lead of major US internet service providers, such as AT&T, Verizon, Google, Facebook or Twitter, and

proactively reports on the frequency of law enforcement requests and how they respond to them.

Routing transparency is almost entirely absent

Fewer than half (8/20) of the ISP privacy policies refer to the location and jurisdiction for the information they store. Only one (Hurricane), gives an indication of where it routes customer data and none make explicit that they may route data via the US where it is subject to NSA surveillance.[28] This is part of a more general pattern of not providing specific information publicly, instead placing the burden on individuals to make specific enquiries.

ISPs rely heavily on implied consent

Many of the privacy policies evaluated contain buried "catch-all" language relating to implied consent. For example, Bell's privacy policy (p. 8) notes:

> *In general, the use of products and services by a customer, or the acceptance of employment or benefits by an employee, constitutes implied consent for the Bell companies to collect, use and disclose personal information for all identified purposes.*

POLICY RECOMMENDATIONS

Without proactive public reporting on the part of ISPs in the key areas identified above, it is very difficult for Canadians to protect their personal privacy nor hold these important organizations to account. To remedy this situation, we make the following recommendations directed at the primary internet privacy actors:

Recommendations for ISPs/carriers that handle Canadian internet traffic.

ISPs should go beyond minimum compliance with Canadian privacy law, and, in the spirit of PIPEDA's Principle 8 – Openness, commit proactively to making the information identified by the ten criteria readily available on their corporate websites. In particular, this proactive process should include publishing on the privacy sections of their websites:

Recommendation 1: A public commitment to PIPEDA compliance

All ISPs that handle Canadian internet traffic should prominently display a public commitment to compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). This should include reference to the Act itself. They should make explicit the implicit requirement that to the extent feasible any other carrier they hand personal data to provides comparable privacy protection. (See also Recommendations 7 & 8)

Recommendation 2: A public commitment to inform users when personal data has been requested by a third party

All ISPs that handle Canadian internet traffic should prominently display a public

28. It is worth noting that personal information that is kept within Canadian jurisdiction is also subject to state surveillance activities; however, Canadian entities conducting surveillance within Canada are subject to Canadian law and its Constitution. Should Canadians determine that the Canadian surveillance apparatus is to change, that would possibly affect the level of surveillance on intra-Canadian traffic. The same cannot be said about traffic that passes through the US and other foreign countries as Canadians cannot easily force change in the laws and surveillance practices of foreign countries.

commitment to notify customers in a timely way when their personal data has been requested by a third party, unless otherwise prohibited by law. Website text could read:

> *<This company>'s policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order. Law enforcement or security agency officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other process that specifically precludes customer notification.*

Recommendation 3: Regular detailed transparency reporting that provides information about third party data requests and disclosures

All ISPs that handle Canadian internet traffic should publish transparency reports every year or more often. These reports should include information about the requesting entities, including their country of origin, the specific agency or organization, the legal authority for the request and purpose for the request. For all such disclosure or transfer requests complied with, ISPs should provide relevant justifications. Reporting should include the numbers of requests, the number of accounts covered, the number of requests fully and partially complied with, the number declined, and the number of accounts implicated. These transparency reports should be easily accessible via the web as well as downloadable for easy sharing and analysis. Those ISPs that want to lead by example should also commit to related public education campaigns by creating whole sections of their websites devoted to these reports and include additional explanatory materials, such as videos and supplementary documents where possible.

Recommendation 4: Detailed conditions and procedures for law enforcement and other third parties that submit requests for personal information

All ISPs that handle Canadian internet traffic should make public clear guidelines for law enforcement and other third parties to follow when making requests for personal information. A suitable way to do this is through publishing law enforcement agency (LEA) handbooks.

The Guidelines for Law Enforcement, posted by Twitter provide a good model to follow: https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#9

Recommendation 5: A clear indication that metadata and device identifiers are included in the definition of 'personal information'

All ISPs that handle Canadian internet traffic should make publicly clear that they include communication meta-data as well as persistent unique devices identifiers among the personal information they protect under Canadian privacy law. Since metadata is a broad term, they should itemize specifically the items comprising the metadata that they collect.

Recommendation 6: Retention periods and the justification for these, for the various types of personal information handled

All ISPs that handle Canadian internet traffic should provide details about retention periods for the various types of personal information it handles. Justifications for these retention periods should be provided. Many ISPs have determined internally how long they will hold onto certain types of data. This information must be made public. For example:

"The following is a list of types of personal information that we retain and the normal retention periods for each type of data:

IP logs: x days;
call records: y days;
preservation requests: 90 days.

In case of legal proceedings, we may be required to retain personal data until the litigation is concluded."

Recommendation 7: Details of whether personal data may be stored or routed outside Canada

All ISPs that handle Canadian internet traffic should provide detailed information about the location of storage and routing of personal data. This includes listing, for example:

- the countries through which data is routinely routed;
- the countries where data is stored,
- the jurisdictional authority of all the carriers it exchanges traffic with,
- an explicit indication of whether these carriers provide data protection comparable to that expected under Canadian law.

Recommendation 8: How they strive to keep Canadians' data within Canadian legal jurisdiction

All ISPs that handle Canadian internet traffic should make public the measures they adopt to keep Canadians' data and domestic internet traffic within Canadian legal jurisdiction, or at least protect it from foreign jurisdiction, particularly the US. These measures could include:

- storing data within Canada,
- exchanging traffic only with carriers providing data protection comparable to that expected under Canadian law,
- exchanging traffic at public internet exchange points in Canada,
- encrypting traffic when unavoidably subject to foreign jurisdiction, with the keys kept with the individual subscriber or within Canadian legal jurisdiction

Recommendation 9: How they strive to keep Canadians' data protected against mass Canadian state surveillance

All ISPs that handle Canadian internet traffic should make public, to the extent legally permissible, their relations with Canadian law enforcement and security agencies, as well as the measures they adopt to protect data against access by these agencies without legal due process and oversight.

Recommendation 10: The extent to which they advocate for their subscribers' privacy rights.

All ISPs that handle Canadian internet traffic should clearly indicate their stance on current related to personal data privacy protection and mass state surveillance. This stance should include their position on alleged NSA and CSEC surveillance of Canadian internet transmissions. If an ISP is making official submissions or lobbying in relation to any prospective legislative, regulatory or policy change that can influence subscriber data

protections, its activities should be readily available on its privacy pages. An ISP should be similarly transparent if it is involved in any court case around the privacy rights of their subscribers. Whatever the ISPs position in relation to user privacy rights, this should be made publicly clear.

Recommendation for Privacy Commissioners and the Canadian Radio-Television and Telecommunications Commission (CRTC).

Recommendation 11: Regulators should more closely oversee ISPs to ensure their data privacy transparency

Both the Office of the Privacy Commissioner (OPC) and Canadian Radio-Television and Telecommunications Commission (CRTC) have responsibilities under their respective legislative mandates to ensure that ISPs are respecting the privacy of their subscribers. They should exercise their powers more vigorously, to ensure proper handling of personal information and in particular that ISPs only hand off internet traffic to carriers that meet Canadian privacy law standards.

Recommendation for legislators and politicians.

Recommendation 12: Amend PIPEDA's Principle 8 — Openness to include public transparency.

In particular it should be amended as follows:

> *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 to inserted text)*

Recommendation 13: Amend PIPEDA's Principle 9 — Individual Access to require proactive notification

Currently Principle 9 only requires organizations to respond to individual requests. It should be amended to require timely proactive notification to the individual whenever a third party requests disclosure of their personal information. Any exceptions should be limited, specific and justified in relation to the circumstances.

Recommendation for Canadian law enforcement and security agencies

Recommendation 14: Canadian law enforcement and security agencies should proactively publish statistics about requests for personal information they make to ISPs

Just as leading internet businesses are beginning to do, the law enforcement and security agencies that request ISPs to disclose personal customer information should routinely and proactively publish detailed statistics about their requests, the rationales, ISP responses, and how these have assisted or not in achieving their mandates.

This report calls on ISPs, regulators, legislators, law enforcement and security agencies to remove the systemic barriers to data privacy transparency, and to implement a more proactive approach requiring robust public transparency norms.

These various measures advancing data privacy transparency will contribute to ensuring that ISPs and third party data requestors are accountable to the public and the spirit of Canadian privacy law for their data management practices. Those actors adopting strong transparency measures will demonstrate leadership in the global battle for data privacy protections, and help bring state surveillance under more democratic control.

APPENDIX: ISP PROFILES AND EVALUATIONS

Following are the details of our evaluations for each of the 20 ISPs in our selected sample of leading telecommunications carriers providing intra-Canadian internet routing services. Each entry includes a table showing scores for each of the 10 criteria, with explanatory footnotes. Also included are:

- A brief overview of the carrier,
- The location of corporate headquarters, indicating their primary national jurisdictional affiliation and responsibility,
- The carriers' Autonomous System Number (ASN), a globally unique number associated with a network operator that presents a common, clearly defined **routing policy** to the Internet. The ASN number is used to identify particular ISPs from routing data, and
- Autonomous System Number (ASN) rank, as published by CAIDA – The Cooperative Association for Internet Data Analysis in late 2013. ASN rankings give an indication of the relative size of a carrier in terms of its routing connections and capacity. See: **http://as-rank.caida.org**.

ABOVENET COMMUNICATIONS (ZAYO)

Headquarters: Louisville, Colorado, USA **ASN:** 6461
Corporate Site: www.zayo.com/abovenet **AS Rank:** 19

AboveNet is a telecommunication service provider focusing primarily on Ethernet services for corporate clients. They offer access speeds approaching 10Gbps, noting "AboveNet minimizes or eliminates the clutter of other connectivity solutions by connecting your enterprise metro location via this Ethernet service."[29] In 2012, AboveNet was purchased by the Zayo Group. Their corporate website describes their 'complete' North American footprint, strong presence in Europe, serving 208 metro markets, seven countries and more than 61,000 route miles. They also have "a comprehensive portfolio of transport, dark fiber, colocation, and IP services".[30]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): Zayo's Privacy Policy [1]

[1] Zayo's privacy policy is one page and only addresses data collected from their corporate website.

29. http://www.above.net/products/metroenet.php
30. http://www.zayo.com/abovenet

AMERICAN TELEPHONE AND TELEGRAPH (AT&T)

Headquarters: Dallas, Texas, USA **ASN:** 7018
Corporate Site: www.att.com **AS Rank:** 14

AT&T is one of America's oldest and largest telecommunications companies. AT&T offers "one of the world's most advanced and powerful global backbone networks, carrying 49 petabytes of data traffic on an average business day to nearly every continent and country". AT&T is also a leading worldwide provider of IP-based communications services, mobile and fixed-line telephone service and claim to offer "the nation's (U.S.) fastest and most reliable 4G LTE network". AT&T also claims to have "the largest international coverage of any U.S. wireless carrier of any U.S. wireless carrier", and "the nation's largest Wi-Fi network including more the 32,000 AT&T Wi-Fi Hot Spots … and provide access to more than 461,000 hotspots globally through roaming agreements".[31]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	YES/NO[2]
4) Transparency about conditions for third party data disclosures	YES/NO[3]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[4]
7) Publicly states where personal information is stored.	YES/NO[5]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): AT&T's Privacy Policy Page

[1] AT&T has an overarching privacy policy that apparently applies to "to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors"; however, the privacy policy does not reference PIPEDA or Canadian privacy law in any way.

[2] AT&T has recently issued it's first Transparency Report,[32] but doesn't provide nearly as much detail as reports from other internet providers. In particular, it doesn't provide details on Canadian requests, nor on Canadians implicated in US national security and law enforcement demands.

31. http://www.att.com/gen/investor-relations

32. http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

[3] Indicates a variety of instances where data sharing will take place with/without consent, as well as instances where data will not be shared/sold. For example,

> *There are also occasions when we provide Personal Information to other companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to: Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims.*

Half-star is awarded because description uses the phrase "some examples include" as opposed to providing an exhaustive list.

[4] AT&T does not provide details, noting instead, "We keep your Personal Information as long as we need for business, tax or legal purposes."

[5] Indicates personal data may be stored or processed outside the United States, but does not specify which countries.

BELL CANADA

Headquarters: Verdun, Quebec, Canada
Corporate Site: WWW.BELL.CA
ASN: 577
AS Rank: 81

Bell Canada is "Canada's largest communications company." It offers national high speed and wireless Internet services for residents and businesses, cloud computing services, satellite TV and digital television, and landline telephone and mobile phone services; the latter through its Bell Mobility, SOLO and Virgin Mobile Canada brands.[33]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES[1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	YES/NO[4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Bell's Privacy Policy**[5]

[1] PIPEDA reference:

> *The Bell Privacy Policy reflects the requirements of the Personal Information Protection and Electronic Documents Act and incorporates the ten principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which was published in March 1996 as a National Standard of Canada.*

[2] Information about disclosure conditions:

> *The Bell companies may disclose personal information without knowledge or consent to a lawyer representing the companies, to collect a debt, to comply with a subpoena, warrant or other court order, or as may be otherwise required by law.*

33. http://www.bce.ca/aboutbce/bellcanada/residentialservices/

[3] Insufficient information about retention periods:

> *The Bell companies shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected.*

They also note without providing sufficient detail:

> *The Bell companies shall maintain reasonable and systematic controls, schedules and practices for information and records retention [...]*

[4] Information about data storage:

> *In some cases, personal information collected by the Bell companies may be stored or processed outside of Canada to provide you with the service or to support Bell operations, and may therefore be subject to the legal jurisdiction of these countries.*

[5] Privacy Policy was updated in May 2011.

BELL ALIANT

Headquarters: Halifax, Nova Scotia, Canada **ASN:** 855
Corporate Site: WWW.BELLALIANT.NET **AS Rank:** 523

Bell Aliant is a Canadian telecommunications provider, serving Canadians throughout Atlantic Canada and in select regional markets in Ontario and Quebec.[34] Bell Aliant was created in 1999[35] "by joining Bell Canada's regional wireline business in Ontario and Quebec, Bell's majority interest in Bell Nordiq, the Aliant wireline business in Atlantic Canada."[36] Bell Aliant offers telephone, "data, Internet, video and value-added business solutions."[37]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES[1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	YES/NO[4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO[5]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Bell Aliant's General Security and Privacy homepage**; **General Security page**; **General Privacy page**; **General Code of Fair Information Practices page**; **FibreOP Privacy and Security homepage (Ontario)**; **FibreOP Security Page (Ontario)**; **FibreOP Code of Fair Information Practices page (Ontario)**

[1] PIPEDA reference:

> *The Privacy Policy and the Code of Fair Information Practices spell out the commitments of The Company and the rights of customers regarding personal information. They also comply fully with the Personal Information Protection and Electronic Documents Act, which is effective January 1, 2001.*

34. "Bell Aliant: Regions We Serve," accessed May 24, 2013, **http://bellaliant.ca/english/about/regions.shtml**.
35. "Bell Aliant Timeline," accessed May 24, 2013, **http://www.bellaliant.ca/english/about/popup_timeline8.html**.
36. "About Bell Aliant," accessed May 24, 2013, **http://bellaliant.ca/english/about/index.shtml**.
37. "Bell Aliant News," accessed May 24, 2013, **http://bell.aliant.ca/english/news/view_art.asp?id=2217**.

[2] Information about disclosure conditions:

> *While our general policy is not to provide personal information to any party outside of Bell Aliant, there are certain limited circumstances [...] in which it is necessary to do so. [...] Third parties include ... Law enforcement agencies, in emergencies, for internal security matters, or where required by court order or search warrant [...]*

[3] Insufficient information about retention periods:

> *In all cases, information is retained in secure facilities, protected from unauthorized access and kept only as long as is reasonably required. [...] We will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the customer or as required by law. The Company will retain personal information only as long as necessary to fulfill those purposes.*
>
> *The Company shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law.*
>
> *The Company shall maintain reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained*

[4] Information about data storage:

> *Personal information is usually stored and processed in Canada. However in limited cases, personal information we collect may be stored or processed with service providers outside of Canada, and may therefore be subject to the legal jurisdiction of these countries. These service providers are given the information they need to perform their designated functions, and we do not authorize them to use or disclose personal information for their own marketing or other purposes. The information is also protected with appropriate security safeguards.*

[5] Has a public presence at TorIX, but peers conditionally.

COGENT COMMUNICATIONS

Headquarters: Washington, DC, USA
Corporate Site: WWW.COGENTCO.COM
ASN: 174
AS Rank: 2

Cogent Communications is a multinational Internet service provider, with subscribers in more than 36 countries and 180 markets.[38] Founded in 1999, Cogent is headquartered in Washington, D.C. and offers Internet access, data transport and colocation services. Cogent Canada, Inc. based in Toronto, Ontario was established in 2002, and Canadian services are available in Vancouver, Toronto, Hamilton, and Montreal. Cogent is one of the "top five global service providers in the world" and is "widely recognized as one of the largest carriers of Internet traffic in the world."[39]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO[2]
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Cogent Acceptable Use Policy**

[1] Cogent does not have an official privacy policy. At the end of its acceptable use policy it notes,

> *Cogent makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Cogent technology, and makes no guarantee that any other entity or group of users will be included or excluded from Cogent's network.*

[2] Cogent does provide access to a Looking Glass service on its website; however, no clear information about the routing of Canadian traffic is noted (**http://cogentco.com/en/network/looking-glass**)

38. "Cogent: History," accessed May 24, 2013, **http://www.cogentco.com/en/about-cogent/history**.

39. "About Cogent," accessed May 24, 2013, **http://www.cogentco.com/en/about-cogent**.

DISTRIBUTEL

Headquarters: Ottawa, Ontario, Canada
Corporate Site: WWW.DISTRIBUTEL.CA
ASN: 11814
AS Rank: 6584

Distributel Communications is an Ottawa, Ontario-based[40] company offering high speed Internet services, telephone services and long distance plans to residents of British Columbia, Alberta, Ontario, and Quebec.[41] Distributel began in 1988, as "one of the pioneers of the competitive long-distance industry in Canada."[42]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES[1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES[4]
10) Open advocacy for user privacy rights (such as in court/legislatively)	YES/NO[5]

Primary Source(s): **Distributel Privacy Policy**[6]; **Bogart, N. (11 Feb 2013). Globalnews.ca**

[1] PIPEDA reference:

> *Distributel is fully compliant with federal legislation that has been designed to protect you and your personal information. We have based our privacy policy on the 10 standard Privacy Principles included in Schedule 1 of the Personal Information Protection and Electronic Documents Act, also referred to as P.I.P.E.D.A.*

[2] Distributel does note in its privacy policy that data disclosure is "pursuant to a legal power"; however, their transparency in this regard is far too brief to earn any stars for this criterion.

[3] Insufficient information about retention periods:

> *We will retain your personal information only long enough to satisfy the purpose(s) to which you have already consented. Within a reasonable time after the purpose has been satisfied, your sensitive information will be destroyed or made anonymous.*

40. "Contact Us | Distributel," Distributel.ca, accessed May 24, 2013, **http://www.distributel.ca/en/contact.aspx**.

41. "About Us | Distributel," Distributel.ca, accessed May 24, 2013, **http://www.distributel.ca/en/aboutus.aspx**.

42. Ibid.

[4] Peers unconditionally at TorIX.

[5] Noted in **Bogart, N. (11 Feb 2013). Globalnews.ca** If this privacy advocacy was identified on the company website, it would receive a full star.

> *Independent Canadian ISP Distributel is opposing a motion to disclose the identities of some of its subscribers who are alleged to have been involved in file sharing.*

[6] Privacy policy last updated in 2010.

EASTLINK

Headquarters: Halifax, Nova Scotia, Canada **ASN:** 11260
Corporate Site: WWW.EASTLINK.CA **AS Rank:** 6584

Eastlink provides telecommunications, entertainment, and advertising services to residents of "Atlantic Canada, Ontario, Quebec, Alberta, Manitoba, British Columbia and Bermuda."[43] Telecommunications services include high speed Internet, HD and OnDemand television, and residential telephone services; locally-produced television content is available via Eastlink TV. Founded in 1970 and owned by Bragg Communications,[44] Halifax, Nova Scotia-based Eastlink is the "the largest, privately held telecommunications company in the country and the fifth largest teleco overall in Canada."[45]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES[1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	NO[4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO[5]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Eastlink Privacy Policy**; **Eastlink Code of Fair Information Practices**

[1] PIPEDA reference:

> *Eastlink's Code and Policy were developed to be fully compliant with the federal government's privacy legislation, the Personal Information Protection and Electronic Documents Act ("PIPEDA").*

[2] Information about disclosure conditions:

> *While our general policy is not to provide personal information to any party outside of Eastlink without your consent, there are certain limited circumstances in which it is necessary to do so. […] where the customer consents to such disclosure or disclosure is required by law. (Privacy Policy) Eastlink may disclose a customer's personal information to: […] law enforcement agencies and other parties with a court order (CFIP)*

43. http://www.eastlink.ca/About.aspx.
44. http://www.manta.com/ic/mt6l1qn/ca/bragg-communications-incorporated.
45. http://www.eastlink.ca/About/History.aspx.

[3] Insufficient information about retention periods:

> *Eastlink shall retain personal information only as long as necessary for the fulfillment of the identified purposes. .. Eastlink shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law. Eastlink has a records retention policy that specifies the length of time that records are maintained. Personal information that has been used to make a decision about an individual is retained long enough to allow the individual access to the information after the decision has been made.*

[4] Brief reference in Terms of Service statement, but no reference in Privacy/CFIP statements.

[5] Has a public presence at TorIX, but peers conditionally.

HURRICANE ELECTRIC INTERNET SERVICES

Headquarters: Fremont, California, USA **ASN:** 6939
Corporate Site: www.he.net **AS Rank:** 10

Hurricane Electric is a "global IPv4 and IPv6 network and is considered the largest IPv6 backbone in the world as measured by number of networks connected."[46] They are connected to 60 internet exchange points around the world and exchange traffic directly with more than 2,800 networks. They also own and operate two data centres in Fremont, CA.

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	YES/NO[3]
9) Take publicly visible steps to avoid US routing of Canadian data	YES[4]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): http://www.he.net/about_legal.html; http://www.he.net/about_network.html; http://www.he.net/news.html

[1] Noted in Terms of Service agreement:

> *Hurricane Electric will use its best efforts to maintain, but does not guarantee, the privacy of email, network use, and the contents of user directories.*

[2] Information about disclosure conditions:

> *Hurricane Electric will not disclose any information about any individual user except to comply with applicable law or valid legal process, or to protect the personal safety of our users or the public. Hurricane Electric may disclose any information about their users under special circumstances that include but are not limited to complying with the law, or assisting in rectifying an unjust doing.*

[3] Transparency about storage and routing of personal information. On Hurricane's 'About' page they note that they have "no less than four redundant paths crossing North America, two separate paths between the U.S.

46. http://www.he.net/about_us.html

and Europe, and rings in Europe and Asia." 'Network Information' link brings users to a detailed network map. They also provide additional peering information, and a network looking glass. This is not sufficiently clear to inform Canadians that their data may be subject to U.S. routing and jurisdiction, thus we only award a half-star.

[4] Peers unconditionally at TorIX.

LEVEL 3 COMMUNICATIONS

Headquarters: Broomfield, CO, USA
Corporate Site: www.level3.com
ASN: 3356
AS Rank: 1

Level 3, a Colorado-based telecommunications company, claims to be one of the "world's top three Internet traffic carriers,"[47] and one of only six Tier 1 Internet providers globally.[48] In 2011, Level 3 and the ISP Global Crossings merged giving the new company access to "more than 500 global markets in North America, EMEA, Latin America and Asia, as well as a total of ~100,000 route miles." Level 3 notes that its current Canadian ISP vendors are Bell, Shaw, Rogers, MTS Allstream, Telus and Hydro One.[49]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO[1]
5) Publicly states an explicitly inclusive definition of 'personal information'	YES/NO[2]
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	NO[4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **http://www.level3.com/en/privacy**

[1] Level 3 notes,

> *We reserve the right to disclose your personally identifiable information as explicitly set forth in this Privacy Policy or any user agreement agreed to by you, or as otherwise required by government or law enforcement officials. We can, and you hereby authorize us to, disclose any information to law enforcement or other parties that we in our sole discretion, believe is required or appropriate to comply with the law.*

[2] Level 3's online privacy policy only refers to "our websites or our audio, conferencing and on-line services". It does not clearly state that it applies to personal data carried over its networks. For this reason, its fairly long

47. http://www.level3.com/en/about-us/company-information/company-history/
48. http://www.level3.com/en/about-us/
49. http://www.level3.com/~/media/Assets/fact_sheets/fact_sheet_canada.ashx

description of 'personal identifiable information' only receives a half-star.

[3] Insufficient information about retention periods:

> *The length of time we keep your information for can vary according to how we use that information. Unless there is a specific legal requirement to keep your information, we will not keep it for longer than we believe is reasonably necessary for the purposes for which the data was collected.*

[4] Information about data storage:

> *We are a multinational group of companies and the information that we collect from you may be shared with Level 3 affiliate companies in locations around the world. [...] Users from the EEA should note that we may transfer personally identifiable information to countries outside of the EEA where we, or our subcontractors, may store and process it.*

MTS ALLSTREAM

Headquarters: Winnipeg, Manitoba, Canada **ASN:** 15290
Corporate Site: www.mts.ca **AS Rank:** 151

MTS Allstream is a Winnipeg, Manitoba-based telecommunications company delivering high speed Internet, wireless, digital TV, converged IP networking, and residential telephone services.[50] The company's core business units include Allstream, a national business-focused communications provider, and MTS, which provides residential and business telephone and Internet services in Manitoba.[51] The company is the fourth-largest communications provider in Canada.

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES[1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO[2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO[3]
7) Publicly states where personal information is stored.	YES/NO[4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO[5]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **MTS Allstream Privacy Code**

[1] PIPEDA reference:

> *The application of the Company's Privacy Code is subject to the requirements or provisions of Part I of the Personal Information Protection and Electronic Documents Act, the regulations enacted thereunder, and any other applicable legislation or regulation, including any applicable regulations of the Canadian Radio-television and Telecommunications Commission and the requirements of any applicable legislation, regulations, tariffs or agreements, such as collective agreements, or the order of any court, or other lawful authority.*

[2] Information about disclosure conditions:

> *The Company may also collect, use and disclose personal information without knowledge or consent if: a) seeking the consent of the individual might defeat the purpose of collecting the*

50. "Corporate Profile | MTS," accessed May 24, 2013, **http://www.mts.ca/mts/about+mts+allstream/our+company/corporate+profile**.

51. "Our Business | MTS," accessed May 24, 2013, **http://www.mts.ca/mts/about+mts+allstream/our+company/our+business**.

information, such as in the investigation of a breach of an agreement or a contravention of a federal or provincial law; b) there is an emergency where the life, health or security of an individual is threatened; or c) disclosure is to a lawyer representing the Company, to collect a debt, to comply with a subpoena, warrant or other court order, or otherwise required or permitted by law.

[3] Insufficient information about retention periods:

The Company shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected. […] For safety, security and liability purposes, the Company may use cameras in its retail stores and adjoining areas such as exterior hallways and parking lots. Information recorded by such cameras is retained for a short period, unless needed in conjunction with an investigation. […] The Company shall maintain reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained.

[4] Information about data storage:

When outsourcing certain business or operational functions, the Company strives to minimize the personal information stored or processed outside of Canada. However, in some cases, personal information may be stored or processed outside of Canada to provide customer or employees with service or to support the Company's operations, and therefore may be subject to the legal jurisdiction of such non-Canadian territory.

[5] Has a public presence at TorIX, but peers conditionally.

PEER 1 HOSTING

Headquarters: Vancouver, BC, Canada
Corporate Site: www.peer1.com
ASN: 13768
AS Rank: 152

PEER 1 Hosting is a global web hosting company, specializing in "Managed Hosting, Dedicated Hosting, Colocation, Cloud Hosting and Network Services."[52] Launched in 1999 and based in Vancouver, British Columbia, PEER 1 is now a subsidiary of Cogeco Cable.[53] PEER 1 offers 20 state-of-the-art datacenters and 10 colocation facilities across Europe and North America.

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO [2]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO [3]
5) Publicly states an explicitly inclusive definition of 'personal information'	YES/NO [4]
6) Publicly states the normal retention period for personal information	YES/NO [5]
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO [6]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **PEER 1 Privacy Policy**; **Master Services Agreement (Terms and Conditions)**[7]

[1] Privacy policy only applies to Peer 1's website. Terms of service agreement has slightly more information about other internet services.

[2] Though Peer 1 states the following, it does not reference Canada or Canadian policy in its privacy policy:

> *Peer 1 complies with the US-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and rention (sic) of personal information from European Union countries.*

The following is noted in Peer 1's Terms and Conditions:

> *With respect to Services rendered by PEER 1 in Canada, this Agreement will be governed by, and construed in accordance with, the laws of Canada and all disputes arising out of or related to this Agreement will be brought exclusively in the courts located in the Province of British Columbia;*

52. "PEER 1 Hosting Fact Sheet | PEER 1 Hosting," accessed May 24, 2013, http://www.peer1.ca/why-peer-1/peer-1-hosting-fact-sheet.

53. "PEER 1 Hosting Extends PCI Compliance Accreditation," accessed May 24, 2013, http://www.peer1.ca/news-update/peer-1-hosting-extends-pci-compliance-accreditation.

provided, however, that neither party will be prevented from enforcing any related judgment against the other party in any other jurisdiction.

[3] Insufficient information about disclosure conditions:

Users should understand that adherence to the Safe Harbor Privacy Principles may be limited to the extent necessary to meet national security, public interest, law enforcement requirements, judicial process or if the effect of the EU Directive or of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

[4] The following only applies to PEER 1's website:

Peer 1 may collect various types of personal data voluntarily provided by Users, including name, company name, address, telephone number, credit card number or other billing information, e-mail address, and other information such as survey responses. Peer 1 may also collect information about how Users use this Website, for example, by tracking the number of unique views received by the pages of the Website or the domains from which Users originate.

[5] Information about retention periods:

PEER 1 makes no guarantees about retaining any data stored on PEER 1's systems or servers following expiration or termination of this Agreement. PEER 1 will typically delete such data (a) seven days following termination of any PEER 1 Managed Hosting Services by either you or PEER 1 or (b) on your next billing date following termination of any PEER 1 Dedicated Hosting (ServerBeach) Services by either you or PEER 1. You will not have access to your data stored on PEER 1's systems or servers during a suspension or following a termination.

[6] Has a public presence at TorIX, but peers conditionally.

[7] Last updated in 2009

PRIMUS TELECOMMUNICATIONS (CANADA)

Headquarters: Herndon, Virginia, USA
Corporate Site: www.primus.ca
ASN: 6407
AS Rank: 1366

Primus Telecommunications is a global carrier and Canada's "largest alternative telecommunications service provider". Primus is described as offering "a wide selection of consumer and business telecommunications services available nationwide (Canada) including Home Phone, Internet, Long Distance, VoIP, Wireless, Hosting, Managed Services and Enterprise IP Telephony."[54]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO [2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO [3]
6) Publicly states the normal retention period for personal information	NO [4]
7) Publicly states where personal information is stored.	YES/NO [5]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES [6]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): http://primus.ca/index.php/ont_en/privacy-policy; http://wireless.primus.ca/privacy[7]

[1] PIPEDA reference:

> *Primus Canada's Privacy Policy is enacted pursuant to the Personal Information Protection and Electronic Documents Act§, and is effective as of January 1, 2001.*

[2] Information about disclosure conditions:

> *Primus Canada may provide personal information to its lawyer or agent to collect a debt, comply with a subpoena, warrant or other court order, government institution requesting the information upon lawful authority, or as may be otherwise required by law.*

[3] Only refers to Primus' website. While Primus indicates that it uses customers' IP addresses, it does not include IP address within the scope of the 'personal information' that is protected under PIPEDA. Noted on the Wireless Privacy Policy page:

> *We use your IP address to help diagnose problems with our server and to understand which pages users access most frequently. Your IP address is also used to gather broad demographic information in an aggregated form.*

54. http://primus.ca/ont_en/about-us

[4] Insufficient information about retention periods:

> *Primus Canada will retain personal information for only as long as required to fulfil the identified purposes or as required by law.*

[5] Information about data storage:

> *Some of our selected third party service providers/business partners may be located outside of Canada. As a result, your personal information may be accessible to regulatory authorities in accordance with the laws of these jurisdictions.*

[6] Has a public presence at TorIX, but peers conditionally.

[7] Policy revised in 2007

ROGERS COMMUNICATIONS

Headquarters: Toronto, Ontario, Canada
Corporate Site: www.rogers.com
ASN: 812
AS Rank: 158

Rogers Communications is "Canada's largest provider of wireless voice and data communications services."[55] Rogers provides cable television, high speed Internet, residential telephone, and mobile phone services (via its three mobile phone brands, Rogers, Fido, and Chatr).[56]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [2]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO [3]
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO [4]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Rogers Privacy Policy**; **Rogers Privacy FAQ**

[1] Privacy policy last revised in 2006.

[2] PIPEDA reference:

> *Rogers' privacy practices are in accordance with all federal and provincial laws and regulations. We are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA) and where applicable with the privacy rules established by the Canadian Radio-television and Telecommunications Commission (CRTC).*

[3] Insufficient information about retention periods:

> *Rogers retains personal information only as long as necessary for the fulfillment of those purposes.*

[4] Has a public presence at TorIX, but peers conditionally.

55. "News - Rogers Newsroom > Rogers Launches BlackBerry Enterprise Service 10 Version 1 with New Regulated-level EMM Support," accessed May 24, 2013, http://newsroom.rogers.com/news/13-05-14/Rogers_Launches_BlackBerry_Enterprise_Service_10_version_1_with_new_Regulated-level_EMM_support.aspx.

56. "Get to Know Rogers - Media Kit - Rogers Newsroom."

SAVVIS COMMUNICATIONS (CENTURYLINK)

Headquarters: St. Louis, Missouri, USA
Corporate Site: www.savvis.com
ASN: 3561
AS Rank: 25

Savvis provides "IT infrastructure solutions" such as "cloud, colocation and managed-hosting services"[57] to companies around the world. In 2010, Savvis purchased Fusepoint, a Canadian-managed IT and colocation provider, thus establishing a Canadian presence with three data centres in Toronto, Vancouver and Montreal. Savvis merged with CenturyLink, the third largest telecom in the US, in 2011.[58] This merger solidified Savvis' managed hosting and colocation services worldwide, as Savvis/CenturyLink's "combined infrastructure includes 48 data centers in North America, Europe and Asia."[59]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO [2]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO
5) Publicly states an explicitly inclusive definition of 'personal information'	NO [3]
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	YES/NO [4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): http://www.savvis.ca/en-ca/pages/privacy_policy.aspx

[1] No publicly posted privacy policy for data transmission services. Privacy policy only refers to website.

[2] Reference to EU and US policy:

> *Savvis Communications Corporation is committed to following the Safe Harbor Principles for personal information within the scope of the Safe Harbor Privacy Policy.*

[3] Only refers to website:

> *Web server automatically collects information such as the domain name of the service providing you with Internet access, the Internet protocol (IP) address used to connect your computer to the*

57. http://news.centurylink.com/index.php?s=43&item=3072
58. http://www.centurylink.com/Pages/AboutUs/CompanyInformation/
59. http://www.savvis.ca/en-ca/company/pages/history.aspx

Internet, the average time spent on our site, pages viewed, information searched for, access times, and other relevant statistics.

[4] Information about data storage (only refers only to the website):

> *Because Savvis operates from its headquarters in St. Louis, Missouri in the United States of America and through subsidiary companies located in many countries around the globe, and because its Web servers which host its Web sites are located at numerous locations inside and outside the United States, it is possible that personal information about visitors may be transferred from one country to another including in countries where data protection and privacy regulations differ and/or offer different levels of protection. By providing us with your information, you consent to any such transfer of information outside of your country.*

SHAW COMMUNICATIONS

Headquarters: Calgary, Alberta, Canada
Corporate Site: www.shaw.ca
ASN: 6327
AS Rank: 125

Shaw Communications is "a diversified communications and media company" providing broadband cable television, high speed Internet, and residential phone services. Through its various business divisions, Shaw also offers telecommunications and satellite direct-to-home services, and nationally distributed television content through Global Television and 19 specialty channels. Shaw serves 3.4 million Internet and residential phone customers, primarily located in Western Canada.[60]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO [2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	YES/NO [3]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES/NO [4]
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Shaw Privacy Policy**; **http://www.torix.ca/peers.php**

[1] PIPEDA reference:

> *Shaw has established its Privacy Policy in accordance with The Personal Information Protection and Electronic Documents Act.*

[2] Insufficient information about disclosure conditions:

> *Shaw may disclose Customer's Personal Information to [...]a third party or parties, where the Customer has given Shaw consent to such disclosure or if disclosure is required by law, in accordance with The Personal Information Protection and Electronic Documents Act. [...]*
>
> *Except as required or permitted by law, when disclosure is made to a third party other than a Shaw associate or affiliate, or a third party service provider, the consent of the individual shall be obtained and reasonable steps shall be taken to ensure that any such third party has personal information privacy procedures and policies in place that are at least comparable to those implemented by Shaw.*

60. "About Shaw," accessed May 24, 2013, **http://www.shaw.ca/Corporate/About-Shaw/Shaw-Companies/**.

[3] Information about data storage:

> *In the event that a third party service provider is located in a foreign country, Customer and Employee personal information may be processed and stored in such other foreign country. In such circumstances, the governments, courts or law enforcement or regulatory agencies of that country may be able to obtain access to your Personal Information through the laws of the foreign country. Whenever Shaw engages a third party service provider, we require that its privacy and security standards adhere to this Privacy Policy and applicable Canadian privacy legislation.*

[4] Has a public presence at TorIX, but peers conditionally.

TATA COMMUNICATIONS

Headquarters: Mumbai, Maharashtra, India **ASN:** 6453 (ISPA SA)
Corporate Site: www.tatacommunications.com **AS Rank:** 7

Tata Communications is an India-based telecommunications company than controls an underwater cable network, operates a Tier 1 IP network, has connectivity "to more than 200 countries and territories across 400 PoPs, and nearly one million square feet of data centre and collocation space worldwide".[61]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO[2]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	NO
5) Publicly states an explicitly inclusive definition of 'personal information'	NO[3]
6) Publicly states the normal retention period for personal information	NO[4]
7) Publicly states where personal information is stored.	YES/NO[5]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Tata Privacy Policy**; **Web Privacy Policy**

[1] Tata's most visible privacy policy refers only to its website. A different policy referring to data transmitted over its networks (which span the globe) appears on the right side as a PDF icon.

[2] Tata recognizes specific privacy responsibilities for handling personal data of Europeans transmitted to the U.S. While PIPEDA is deemed substantially equivalent to European data protection requirements, there is no such recognition of the need to protect Canadians' data. Noted in the privacy policy referring to the website:

> *TRANSFER OF PERSONAL INFORMATION BETWEEN COUNTRIES Tata Communications may from time to time transfer Personal Information between Countries. When Tata Communications transfers Personal Information between countries of the European Union and the United States, we will insure that the recipient has adequate procedures in place to protect such information. The recipient of Personal Information must either participate in the Safe Harbor program developed by the United States Department of Commerce and the European Union or accept contractual clauses assuring the adequate protection of the Personal Information. Companies which participate in the Safe Harbor program have certified that they adhere to the Safe Harbor Privacy Principles agreed*

61. http://microsites.tatacommunications.com/about/overview.asp

upon by the United States and the European Union. For more information about the Safe Harbor program, please visit the United States Department of Commerce's Safe Harbor web site at URL: www.export.gov/safeharbor

[3] Includes information about IP address collection, but only refers to data collected from its website.

[4] Insufficient information about retention periods:

The Company retains information in accordance with its Records Management Policy which varies according to the nature of the information in question. In some cases, the Company is legally required to retain data for a minimum period of time. In others, there is no proscribed legal retention period.

[5] As noted above, Tata indirectly alerts users that their personal data may be transmitted outside the country of origin. They also add:

When you submit Personal Information to Tata Communications on this Site, you understand and agree that this information may be transferred across national boundaries and may be stored and processed in another country, which may not provide privacy protections similar to those your country provides.

TEKSAVVY SOLUTIONS

Headquarters: Chatham, Ontario, Canada
Corporate Site: www.teksavvy.com
ASN: 5645
AS Rank: 962

TekSavvy is a privately-held Chatham, Ontario-based telecommunications service provider offering Internet and phone services. Founded in 1998, Teksavvy provides residential, business, and wholesale Internet and phone services to select communities in Ontario, Quebec, British Columbia and Alberta and the Maritimes.[62] Teksavvy relies on the "last mile" infrastructure of other carriers including Rogers to deliver its services.[63] Teksavvy's motto is "We're Different. In a Good Way," and the company bills itself as an alternative to the "usual corporate monopolies."[64]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [1]
2) Public commitment to inform users about all third party data requests	YES/NO [2]
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO [3]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO [4]
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	YES [5]
10) Open advocacy for user privacy rights (such as in court/legislatively)	YES/NO [6]

Primary Source(s): **TekSavvy Privacy Policy**; **Copyright FAQ**; **Customer Notices**; **In the News**

[1] PIPEDA reference:

> *[...] the CSA Code was largely incorporated into the Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, as amended ("PIPEDA"). [...] The objective of the Privacy Policy is responsible and transparent practices in the management of personal information, in accordance with the CSA Code and federal legislation.*

62. "TekSavvy - TekSavvy Lowers Prices and Expands Footprint," accessed May 24, 2013, **http://www.teksavvy.com/en/why-teksavvy/in-the-news/teksavvy-press-releases/2013-press-releases/teksavvy-lowers-prices-and-expands-footprint**.

63. "Our Order, In No Particular Order," TekSavvy Blog, accessed May 24, 2013, **http://blogs.teksavvy.com/2012/05/23/our-order-in-no-particular-order/**.

64. "TekSavvy - Who We Are," accessed May 24, 2013, **http://www.teksavvy.com/en/why-teksavvy/company/who-we-are**.

[2] This note is buried in a subsection of TekSavvy's 'In the News' section called 'Legal Documents for Request for Customer information". It only refers to this specific example of data requests:

> *TekSavvy has received a request for customer information from Voltage Pictures LLC. Some of our customers have been notified that an IP address associated with their account has been identified as part of that request. TekSavvy is working to provide our customers all relevant information in this request, including public notices submitted to Federal court and resources to help through the process.*

This is noted in a section entitled 'Copyright FAQ':

> *What is TekSavvy's role when it receives notice of a legal proceeding [...] TekSavvy's role is to ensure that our customers are aware that a request for their personal information has been made so that they have an opportunity to address the court on the matter if they so choose before any disclosure is ordered. [...] How will I know if TekSavvy has received a request for my personal information? TekSavvy will notify you by email and provide as much information it has available about the legal proceeding under which the request is made. [...] How will I know if TekSavvy has disclosed my personal information? TekSavvy will notify affected customers if we receive a court order to disclose their personal information.*

[3] Information about disclosure conditions:

> *The TekSavvy Companies may disclose personal information without knowledge or consent to a lawyer representing the TekSavvy Companies, to collect a debt, to comply with a subpoena, warrant or other court order, or as may be otherwise required by law.*

[4] Insufficient information about retention periods:

> *The TekSavvy Companies shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law. Depending on the circumstances, where personal information has been used to make a decision about a customer or employee, the TekSavvy Companies shall retain, for a period of time that is reasonably sufficient to allow for access by the customer or employee, either the actual information or the rationale for making the decision. [...]*
>
> *The TekSavvy Companies shall maintain reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained.*

In a section labeled Copyright FAQ, TekSavvy includes the following, which would have earned a half-star had it been included in a section relating privacy:

> *Log files identify the IP addresses assigned to TekSavvy customers on an ongoing basis. TekSavvy currently stores log files for 90 days. In cases where legal proceedings are initiated by a holder of copyrights, we may be required to retain the logs until the litigation is concluded.*

[5] Peers unconditionally at TorIX.

[6] Material about recent court cases included. Privacy stance alluded to on site's blog;[65] however, a more recent post about the Canadian government's cyber-bullying bill, which allegedly has similarities with Bill C-30, was described without any mention of privacy implications.[66] While these items are easily found for those looking for them, as they are not identified specifically with the privacy section of the website, it might be difficult for the average user to find them.

65. http://blogs.teksavvy.com/?p=2800

66. http://blogs.teksavvy.com/?p=2835

TELIASONERA

Headquarters: Stockholm, Sweden
Corporate Site: www.teliasonera.com
ASN: 1299
AS Rank: 4

Founded in 1853, TeliaSonera is one of Europe's oldest and largest telecommunications providers, offering fixed-line, mobile and internet services. The company currently has more than 185 million subscribers, and has held Tier 1 network status since 2000.[67]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	NO [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO [2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO [3]
7) Publicly states where personal information is stored.	NO [4]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO [5]

Primary Source(s): **TeliaSonera Privacy Policy**

[1] Privacy policy is not posted on the front page of their website. Instead, it is buried on a page called 'Public Policy' in a section called 'Policy Papers'. While the policy notes "TeliaSonera supports international standards on human rights", it makes no reference to Canada or PIPEDA.

[2] Information about disclosure conditions:

> *TeliaSonera strives to protect the personal data of customers and to safeguard their privacy. We shall therefore: [...] Only provide personal data to authorities to the extent required by law or with the customer's permission. Written demands from authorities are preferable although it is recognised that communications will be oral instead of written in certain circumstances, such as when the law permits verbal demands and in emergency situations.*

[3] Insufficient information about retention periods:

> *TeliaSonera strives to protect the personal data of customers and to safeguard their privacy. We shall therefore: [...] Not retain personal data longer than is legally required or necessary for operational purposes, efficient customer care and relevant commercial activities.*

67. http://www.teliaSonera.com/

[4] Insufficient information about data storage:

> *TeliaSonera strives to protect the personal data of customers and to safeguard their privacy. We shall therefore: […] Process personal data fairly and lawfully in all operations including when processing such data outside the country where it has been collected. […] Expect suppliers to process such data fairly and lawfully in all operations, including when such data is processed outside of the country where it was collected or received.*

[5] On its 'Policy Papers' page, TeliaSonera includes a variety of position and white papers; however, none address privacy specifically, and evidence of a connection to a specific privacy-oriented legislative discussion is unclear. They do note in their privacy policy, that "It is TeliaSonera's objective to live by the letter and spirit of the law".

TELUS

Headquarters: Vancouver, British Columbia, Canada **ASN:** 1299
Corporate Site: www.teliasonera.com **AS Rank:** 4

TELUS is a Canadian telecommunications company, providing over 13.2 million customers with wireless (mobile), residential phone, high speed Internet and TELUS TV services. The company, which is now headquartered in Vancouver, British Columbia, traces its roots back to 1885 when the first Alberta telephone call was made. TELUS is the "second largest telecommunications company" in Canada.[68]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO [2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	NO [3]
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	YES/NO [4]

Primary Source(s): **TELUS Privacy Code**; **Chung, E. (27 Mar 2013) CBC.ca (ADD)**

[1] PIPEDA reference:

> *The TELUS Privacy Code incorporates ten principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (CAN/ CSA-Q830-96). These principles were published in March 1996 as a National Standard of Canada and form the basis of all applicable privacy legislation in Canada, including the Part 1 of the Personal Information Protection and Electronic Documents Act (Statutes of Canada 2000).*
>
> *The TELUS Privacy Code was originally published in 1998 as part of our long-standing commitment to the protection of our clients' and employees' personal information. It was updated in September 2000 to reflect changes associated with the implementation of the federal privacy legislation referred to above, and subsequently updated to comply with applicable provincial privacy legislation where applicable.*

[2] Information about disclosure conditions:

68. "About TELUS - Who We Are," accessed May 24, 2013, **http://about.telus.com/community/english/investor_relations/investor_information/who_we_are**.

TELUS may disclose personal information without knowledge or consent to a lawyer representing TELUS, to collect a debt, to comply with a subpoena, warrant or other court order, or as may be otherwise required or permitted by law.

[3] Insufficient information about data storage:

TELUS may store and process personal information in Canada or another country.

[4] Noted in Chung, E. (27 Mar 2013) Wiretap laws apply to text messages, court rules: Judgment in privacy case overturns lower court ruling against Telus. CBC.ca: (Needs to be on website for full star)

The decision overturns a lower court ruling against Telus Communications that required the company to hand over copies of all the text messages sent and received by two of its customers each day over a two-week period after it was served with a general warrant by police in Owen Sound, Ont.

Telus had appealed the ruling. The phone provider argued that seizing the messages would constitute "interception" of the communication and would therefore require a wiretap warrant.

VIDÉOTRON

Headquarters: Montreal, Quebec, Canada
Corporate Site: www.videotron.com
ASN: 5769
AS Rank: 548

Vidéotron is a Canadian telecommunications company, primarily serving the province of Quebec. A subsidiary of Quebecor Media Inc., Videotron offer services in cable and digital television broadcasting, interactive multimedia development, high speed Internet services, cable telephony and mobile telephone services.[69] The Montreal, Quebec-based company was founded in 1964,[70] and is the Quebec leader in high speed Internet access.[71]

Evaluation of AboveNet	YES/NO
1) Public commitment to PIPEDA compliance	YES [1]
2) Public commitment to inform users about all third party data requests	NO
3) Transparency about frequency of third party data requests and disclosures	NO
4) Transparency about conditions for third party data disclosures	YES/NO [2]
5) Publicly states an explicitly inclusive definition of 'personal information'	NO
6) Publicly states the normal retention period for personal information	NO
7) Publicly states where personal information is stored.	NO
8) Publicly states where personal information is routed.	NO
9) Take publicly visible steps to avoid US routing of Canadian data	NO
10) Open advocacy for user privacy rights (such as in court/legislatively)	NO

Primary Source(s): **Vidéotron Privacy Statement**

[1] PIPEDA reference:

> *Code developed pursuant to the Personal Information Protection and Electronic Documents Act, R.S.C. (2000, c. 5), whose purpose is to establish rules to facilitate the circulation and exchange of information, to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances, and pursuant to the Telecommunications Act, R.S.C. (1993, c. 38)*

[2] Information about disclosure conditions:

> *In certain circumstances, Videotron may Collect, Use, or Disclose Information without the knowledge or consent of the individual concerned. For example, and without limitation: […] In an emergency, when the life, health, or safety of the individual concerned is threatened; In order to collect a debt or comply with a subpoena, warrant, or other court order, or when required by law.*

69. http://corpo.videotron.com/site/our-company/videotron-news/at-a-glance.jsp.
70. http://corpo.videotron.com/site/our-company/history/cable-service-evolution.jsp.
71. http://corpo.videotron.com/site/our-company/videotron-news/facts-numbers.jsp.

ABOUT THE REPORT

Andrew Clement <andrew.clement@utoronto.ca> is a Professor in the Faculty of Information at the University of Toronto, where he coordinates the Information Policy Research Program and is a co-founder of the Identity, Privacy and Security Institute. With a PhD in Computer Science, he has had longstanding research and teaching interests in the social implications of information/communication technologies and participatory design. Among his recent privacy/surveillance research projects, are **IXmaps.ca** an internet mapping tool that helps make more visible NSA warrantless wiretapping activities and the routing of Canadian personal data through the U.S. even when the origin and destination are both in Canada; **SurveillanceRights.ca**, which documents (non)compliance of video surveillance installations with privacy regulations and helps citizens understand their related privacy rights. The SurveillanceWatch app enables users to locate surveillance cameras around them and contribute new sightings of their own; and **Proportionate ID**, which demonstrates through overlays for conventional ID cards and a smartphone app privacy protective alternatives to prevailing full disclosure norms. Clement is a co-investigator in The New Transparency: Surveillance and Social Sorting research collaboration. See **http://www.digitallymediatedsurveillance.ca**.

Jonathan Obar <jonathan.obar@utoronto.ca> is a Postdoctoral Research Fellow in the Faculty of Information at the University of Toronto. He also serves as Visiting Assistant Professor in the Department of Telecommunication, Information Studies, and Media at Michigan State University, and as Associate Director of the Quello Center for Telecommunication Management and Law. Dr. Obar has published in a wide variety of academic journals about the relationship between digital media technologies, ICT policy and the protection of civil liberties.

IXmaps.ca research project:

Since 2008, the **IXmaps.ca** project has worked to help internet users "see where your data packets go", with the aim of raising public awareness of the privacy implications of internet data packet routing. In particular, the project has mapped the sites of likely NSA interception in the US, enabling users to see whether their internet traffic may have been captured. It has also documented the extensive Canadian "**boomerang traffic**" — internet communication that starts in Canada and ends in Canada, but which passes through the US where it is subject to NSA surveillance.

The project has received funding from the **Social Sciences and Humanities Research Council of Canada** and the **Office of the Privacy Commissioner of Canada** and is affiliated with the **New Transparency Project** and the **Information Policy Research Program** at the **Faculty of Information**, **University of Toronto**.