KEEPING INTERNET USERS

IN THE KNOW OR IN THE DARK

Data Privacy Transparency *of* Canadian Internet Carriers

2014 REPORT

Keeping Internet Users in the Know or in the Dark

A Report on the Data Privacy Transparency of Canadian Internet Carriers

Andrew Clement* & Jonathan A. Obar**

andrew.clement@utoronto.ca. jonathan.obar@uoit.ca

IXmaps.ca & New Transparency Projects
*Faculty of Information, University of Toronto
**Faculty of Social Science and Humanities,
University of Ontario Institute of Technology

in collaboration with the Centre for Innovation Law and Policy (CILP),
Faculty of Law, University of Toronto

March 12, 2015

Acknowledgements

We appreciate the contributions of our research collaborators and assistants at the University of Toronto: Antonio Gamba, Alex Goel and Colin McCann. We are also pleased to acknowledge the input of Steve Anderson, (Openmedia.ca), Nate Cardozo (EFF), Andrew Hilts (Cyber Stewards Initiative), Tamir Israel (CIPPIC) and Christopher Parsons (Citizen Lab).

The research reported here benefited significantly from collaboration with the Centre for Innovation Law and Policy (CILP), Faculty of Law, University of Toronto. We worked most closely with Matthew Schuman, Assistant Director, and Ainslie Keith, who led a Volunteer Student Working Group consisting of Shawn Arksey, Michael Cockburn, Caroline Garel-Jones, Aaron Goldstein, Nathaniel Rattansey, Kassandra Shortt, Jada Tellier and Matthew Vaughan.

Website and report design assistance: Jennette Weber

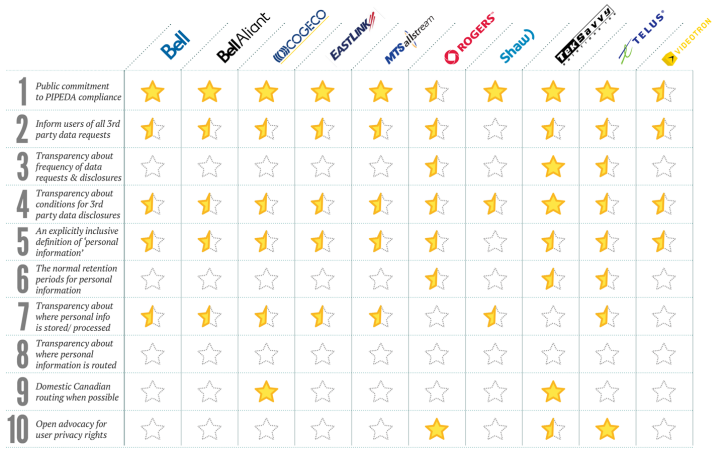
This research was conducted under the auspices of the *IXmaps: Mapping Canadian privacy risks in the internet 'cloud'* project (see IXmaps.ca) and the Information Policy Research Program (IPRP), with the support of the Office of the Privacy Commissioner of Canada (2012-13), *The New Transparency: Surveillance and Social Sorting* project funded by the Social Sciences and Humanities Research Council (2012-15), and *the Mapping Canadian internet traffic, infrastructure and service provision* (2014-15), funded by the Canadian Internet Registration Authority (CIRA).

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

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

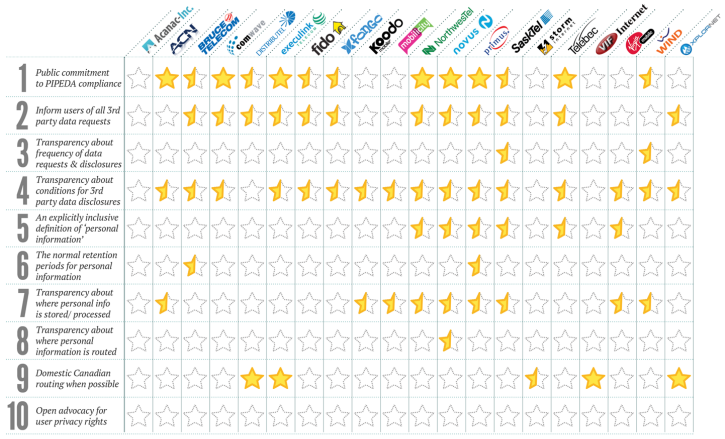
Data Privacy Transparency *of* Canadian Internet Carriers

MAJOR RETAILERS



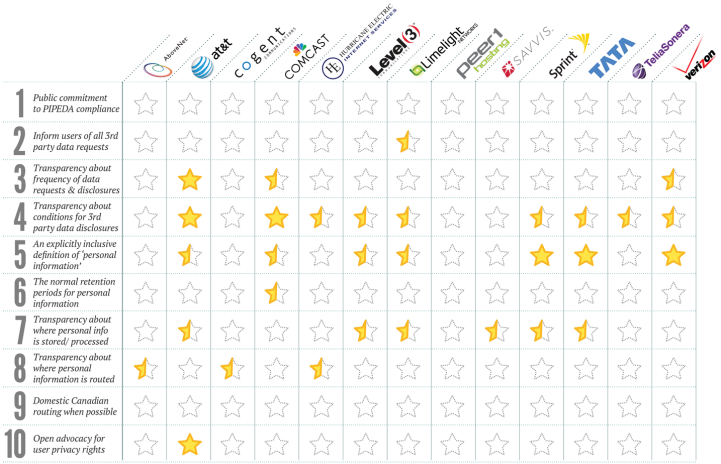
Data Privacy Transparency *of* Canadian Internet Carriers

MINOR RETAILERS



Data Privacy Transparency *of* Canadian Internet Carriers

TRANSIT CARRIERS



Summary

In the wake of the Snowden revelations about mass state surveillance, notably by the US National Security Agency and its Five Eyes partners, there is growing demand for internet carriers to be more forthcoming about how they handle our personal information. Calls for greater privacy transparency in Canada became more urgent after it was revealed that Canadian government agencies are asking telecoms companies to turn over Canadians' user data at "jaw-dropping" rates. Nine carriers received nearly 1.2 million requests in 2011 alone, largely without warrants.[1]

Responding to these concerns, as well as in keeping with the transparency, openness and accountability principles fundamental to Canadian privacy law, this is the second annual report that evaluates the data privacy transparency of the most significant internet carriers serving the Canadian public. We award carriers up to ten 'stars' based on the ready public availability of the following information:

1) *A public commitment to PIPEDA[2] compliance.*
2) *A public commitment to inform users of 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 retentions period for personal information.*
7) *Transparency about where personal information is stored and/or processed.*
8) *Transparency about where personal information is routed.*
9) *Domestic Canadian routing where possible.*
10) *Open advocacy for user privacy rights.*

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.[3] They are also relevant and timely in relation to the landmark *Spencer* Supreme Court of Canada decision that recognized that anonymity on-line is a privacy interest protected by s.8 of the *Charter* and that law enforcement authorities need a warrant to obtain subscriber information from telecoms (*R. v. Spencer 2014 SCC 43)*. This report may also contribute to the debate over several items of federal legislation related to surveillance, privacy and national security that are currently before Parliament.[4]

We awarded stars based on careful examination of each carrier's corporate website. Assuming that carriers want to make it easy for their customers to find information about corporate

---

[1] Alex Boutilier, Government agencies seek telecom user data at 'jaw-dropping' rates, *Toronto Star*, Apr 29 2014.
http://www.thestar.com/news/canada/2014/04/29/telecoms_refuse_say_how_often_they_hand_over_customers_data.html

[2] Personal Information Protection and Electronic Documents Act

[3] Note for instance that the latest incarnation of highly controversial 'lawful access' legislation, Bill C-13 - Protecting Canadians from Online Crime Act, passed into law October 20, 2014.

[4] Current Federal Bills:
S-4 - Digital Privacy Act, 2014
C-44 - Protection of Canada from Terrorists Act, 2014
C-51 - Anti-terrorism Act, 2015

practices relating to personal information, and that the on-line privacy policy page is the first (and likely only) place users might look, we focus our attention on these public statements.[5]

This 2014 report expands the analysis to 43 carriers in our sample based on their prevalence among the approximately 9500 internet traceroutes in the IXmaps.ca database that correspond to intra-Canadian routes – i.e. with origin and destination in Canada. This added several major behind the scenes transit providers that handle internet traffic across the internet 'backbone', typically routing traffic via the US. We also included carriers that are the subject of parallel transparency initiatives.[6] In particular, we were greatly assisted by the Volunteer Student Working Group at the Centre for Innovation Law and Policy (CILP) in the University of Toronto's Faculty of Law. Their companion analysis of six of the most prominent wireless carriers provides valuable detail on the scoring of carriers.[7]

The resulting star ratings can be seen in the accompanying 3 Star Tables:[8]

1 - Major Canadian retail internet carriers
2 - Minor Canadian retail internet carriers
3 - Major international internet transit carriers

The Appendix contains detailed assessments for each carrier. Transparency ratings for particular internet routings and carriers can also be reviewed on the Explore page of the IXmaps website.[9]

Notable Changes from the 2013 Report

While internet carriers generally show little interest in being transparent about key aspects of the handling of personal information, there are some notable improvements over the past year. For the first time a small handful of Canadian carriers have begun issuing their own Transparency Reports, mainly providing statistics about the number of law enforcement requests they receive. While the details in these reports are typically scanty, and not up to the standards being established by large US service providers, this is a good sign that Canadian carriers are beginning to respond to public pressure for greater transparency.

Key Findings

---

[5] 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 main Canadian public internet exchanges, TorIX, OttIX and YYCIX (Toronto/Ottawa/Calgary Internet Exchanges) as these are also publicly visible.

[6] See Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/ and the Access My Info tool, developed by Andrew Hilts of the Digital Stewardship Initiative hosted by Openmedia.ca https://openmedia.ca/myinfo

[7] The 3+3 Project: Evaluating Canada's Wireless Carriers' Data Privacy Transparency, 2014-2015 Centre for Innovation Law and Policy Volunteer Student Working Group, Centre for Innovation Law and Policy (CILP), Faculty of Law, University of Toronto, March 12, 2015. http://innovationlaw.org/3_plus_3

[8] Division into these three tables was based primarily on the difference in role, between Canadian retail ISP and backbone transit carrier, and then secondarily among retail carriers based on the prominence of their internet presence in Canada, rather than their telephone or other service offerings.

[9] http://IXmaps/explore

As the Star Tables make clear, **the internet carriers evaluated are generally not transparent in their handling of personal information**, earning on average only 2 stars out of 10 possible.

No carrier earned a full star in any of these four criteria:

- #2 - A public commitment to inform users of all third party data requests
- #6 - The normal retention periods for personal information
- #7 - Transparency about where personal information is stored and/or processed
- #8 - Transparency about where personal information is routed.

The 'fighting brands' of major mobile carriers, Virgin Mobile, Fido and Koodo, all score below average and are significantly less transparent than their corporate owners, Bell, Rogers and Telus respectively.

Only one company stands out by earning more than 5 stars. TekSavvy achieved 6 stars in aggregate based on full or half stars across eight criteria, the widest spectrum of privacy transparency of any carrier.

For the first time in 2014, Canadian internet carriers have begun issuing Transparency Reports that systematically provide statistics and other relevant details on law enforcement requests for personal data. Rogers, Sasktel, Telus, TekSavvy, and Wind are the pioneers. Some carriers are also being more publically explicit about what they require from law enforcement when making such requests for personal subscriber information.

No transit provider indicates explicit compliance with Canadian privacy law. This is concerning because these behind the scenes internet carriers handle large quantities of intra-Canadian traffic.

Transit carriers generally score much lower than the retail carriers and typically expose personal data to mass state surveillance by the NSA. This is concerning because when outside Canada, or handled by carriers subject to US or other jurisdictions, Canadians' data enjoy no effective legal protection, and certainly much less than when within Canadian jurisdiction[10].

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

---

[10] Lisa M. Austin, Heather Black, Michael Geist, Avner Levin and Ian Kerr, Our data, our laws, *National Post*, December 12, 2013. http://news.nationalpost.com/2013/12/12/our-data-our-laws/
Lisa M. Austin, Enough About Me: Why Privacy is About Power, Not Consent (or Harm) Forthcoming in Austin Sarat, ed., *A World Without Privacy?: What Can/Should Law Do* (Cambridge 2014) http://ssrn.com/abstract=2524512; Lisa M Austin and Daniel Carens-Nedelsky, Jurisdiction still matters: The Legal Contexts of Extra-National Outsourcing, presented at the Assessing Privacy Risks of Extra-National Outsourcing of eCommunications public forum, *Seeing Through the Cloud: Why Jurisdiction Still Matters in a Digitally Interconnected World*, University of Toronto, March 6, 2015. See webcast at: http://mediacast.ic.utoronto.ca/20150306-eComm/index.htm

Recommendations

Without proactive public reporting on the part of carriers in the key areas identified above, it is very difficult for Canadians to hold these important organizations to account. It is also difficult for Canadians to develop the trust in these carriers appropriate to the sensitivity of the information carried in such large volumes. To remedy this situation, we make two primary recommendations:

Primary Recommendation 1:

To demonstrate leadership in the global battle for data privacy protections, to help bring state surveillance under more democratic control, and to earn the trust of Canadians, the companies that carry the personal information of Canadians via the internet need to be much more transparent. This means making clear to Canadians, through comprehensive transparency reports and privacy sections of their websites: who has access to their personal data, on what terms, how long it is kept, where it is stored, processed and routed, and more generally show how they are promoting the privacy interests of their subscribers.

Primary Recommendation 2:

When Canadians' data transits the U.S. or is handled by non-Canadian transit providers, it loses the legal and constitutional protection enjoyed at home. This exposes Canadians to mass suspicionless surveillance by foreign states, especially by the US National Security Agency. In light of this considerable concern, in combination with: a) the general lack of transparency on the part of transit providers and b) across-the-board failure to indicate compliance with Canadian privacy law, Canadian retail carriers should avoid transferring personal data to companies that bring such exposure. This can be achieved by only handing domestic traffic off inside Canada to carriers that operate exclusively within Canadian jurisdiction.

We also offer the following more specific recommendations directed at various key internet privacy actors:

***For carriers* that handle Canadian internet traffic:**

Carriers 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 in a comprehensive privacy section of their corporate websites:

Recommendation 1: A public commitment to PIPEDA compliance, and that data disclosed to third parties for any form of storage, processing or routing should enjoy equivalent protection,

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,

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, processed or routed outside Canada, and what risks this may entail,

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: How they advocate for their subscribers' privacy rights, and

Recommendation 11: Carriers should also consolidate all privacy and transparency policy information so it is easily accessible through the main corporate privacy page.

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

Recommendation 12: Regulators should more closely oversee carriers, Canadian and foreign, to ensure their data privacy transparency and compliance with legal obligations.

For legislators and politicians.

Recommendation 13: Amend PIPEDA's *Principle 8 — Openness* to include proactive transparency around key privacy policies.

Recommendation 14: Amend PIPEDA's *Principle 9 — Individual Access* to require proactive notification in the case of third party disclosure requests.

For Canadian law enforcement and security agencies

Recommendation 15: Canadian law enforcement and security agencies should proactively publish statistics about requests for personal information they make to internet carriers, including the legal basis for such requests and the responses from carriers.

These various measures advancing data privacy transparency will contribute to ensuring that internet carriers 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. They will also earn the trust of Canadians who rely on them for the safe handling of their personal and sensitive data.

Table of Contents

Keeping Internet Users in the Know or in the Dark:

A Report on the Data Privacy Transparency of Canadian Internet Carriers

Introduction

In Canada we entrust the enormous quantities of personal data produced by our online activities to a select group of internet carriers. These carriers, also referred to as internet service providers (ISPs) or telecommunication service providers (TSPs)[11], carry, transmit, and route our data back and forth over the internet between our personal devices (laptops, smartphones, etc.), 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 U.S. National Security Agency (NSA) and Canada's equivalent, Communications Security Establishment (CSE), have secretly gained the cooperation of telecommunications carriers to capture without prior suspicion our data as it flows across their networks, and analyze it for a variety of unknown purposes.

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

This report attempts to make it easier for Canadians to determine just how transparent the carriers they depend on everyday are about privacy matters. We evaluate the most significant internet carriers serving the Canadian public according to 10 criteria, and award them half or full stars based on how well they do. We present the results in 'star tables' to show off the best performers and facilitate comparisons between them. Our hope is both that Canadians will be better informed and equipped to make decisions about their internet service providers, and that carriers will be encouraged to become more transparent about how they handle personal information of millions of Canadians.

The report begins by providing some background on the importance of privacy transparency and reasons for assessing it. We explain how we go about evaluating carriers – which carriers we chose to focus on and why, and then how we apply each of 10 ten criteria to award stars. Based on an analysis of the resulting scores, we identify the most significant findings. These in turn provide the basis of our recommendations, mainly aimed at the carriers, on how they can improve their privacy transparency. An extensive Appendix follows, offering profiles of each of the carriers we rate along with details on their scores.

[11] 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.

Transparency and the "Openness Principle"

The demand 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.*[12]

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[13] and the White House's 2012 Consumer Privacy Bill of Rights.[14] 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.*[15]

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 annual series of reports seeks to overcome the systemic barriers to data privacy transparency in the case of telecommunication service providers. This currently is an area of special concern given the growing evidence of mass state surveillance. As with our 2013 report,[16] we adopt a public accountability approach to examine the privacy materials made public by the 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

[12] http://oecdprivacy.org/
[13] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[14] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[15] http://www.priv.gc.ca/leg_c/p_principle_e.asp
[16] Link to 2013 report

to help Canadians understand better the privacy risks of using the internet and which carriers are more transparent about their privacy practices in which ways.

While this is the first set of Canadian studies of ISP data privacy transparency with broad scope, it is inspired by and contributes to the growing number of similar efforts championing data privacy transparency around the world. These include the Electronic Frontier Foundation (EFF)'s 'Who Has Your Back' reports;[17] and the 'Ranking Digital Rights' Project (led by Rebecca McKinnon of the New America Foundation and University of Pennsylvania).[18] Our study also complements the work of Dr. Christopher Parsons at the University of Toronto's Citizen Lab.[19] Parsons used an in-depth questionnaire approach to make public information that the carriers haven't published proactively. By contrast, and like the EFF, we assess, compare and highlight what ISPs already publicly reveal (or not).

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 do not rate the actual privacy protections carriers offer – that would require a different study – but instead assess a vital ingredient of data privacy and public accountability – transparency. It is quite possible that a carrier may be very protective of our data, but if it is not publicly transparent about its policies and practices, on what basis can we trust it? Given that it is much easier to post statements about privacy policies and practices once formulated than to enact them, the absence of these statements strongly suggests that strong privacy protections don't exist.

We are also not ranking carriers in a single ordering from best to worst. Rather, we prefer to direct attention to specific aspects of privacy transparency, showing where improvement is possible and cheering on those providers that are especially transparent about how they handle our personal information.

Assessing Data Privacy Transparency

We modeled our series of reports 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 digital media service providers more generally (i.e. companies like Apple and Facebook), while broadening the range of criteria to highlight those that are particularly relevant to contemporary privacy concerns in Canada.

---

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

Selecting carriers

This report studies 43 internet carriers, an increase from 20 last year. The primary basis for selecting carriers is not just familiarity to Canadians, but importantly the degree to which they actually carry domestic 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.[20] Currently the database contains over 35,000 traceroutes, of which ~9500 we categorize as intra-Canadian, i.e. they originate and terminate in Canada, whether or not they are routed entirely within Canada. Our studies show that over 20% of domestic Canadian traffic pass through, or transit via the US, in what we refer to as 'boomerang' routing[21]. We examined data on these ~9500 routes for all the ISPs that carried traffic between the immediate origination and destination, and ranked them by the number of routers involved in carrying this traffic.

The resulting selection includes all the major Canadian telecom carriers (Bell, Bell Aliant, Cogeco, 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 also includes those large ISPs that do not have a local, retail presence in Canada but serve as 'transit providers,' handling Canadian traffic behind the scenes, in the 'backbone' or 'core' of the internet. These include a Canadian networking provider (Peer-1, owned by Cogeco), large well known US carriers (AT&T, Comcast, Sprint, Verizon), and major international internet backbone operators (AboveNet, Cogent, Hurricane, Level-3, Limelight, Savvis, Tata and TeliaSonera) that despite their vital role in internet operations, are much less well known publicly. At least one of these latter 12 foreign transit providers is involved in almost every boomerang route in our database. A few of these international giants also route traffic entirely within Canada. This is significant, not only because these transit providers are largely invisible to Canadian consumers, but also because they operate under foreign jurisdictions, usually the US, which can put the data they carry beyond Canadian legal and constitutional protection, even while it is in Canada. Because of their special role in internet operations, we show the star ratings of these 13 carriers in a table of their own – See Star Table 3 Transit Carriers.

While we added four of these foreign transit providers to the carrier list from last year, the largest expansion came from including carriers that were the subject of transparency assessment initiatives conducted in parallel with ours.

In fall of 2014 we were approached by a group of law students affiliated with the Centre for Innovation Law and Policy (CILP) in the Faculty of Law at the University of Toronto wanting to adapt our privacy transparency assessment methods for a study of their own focused on a specific industry sector. Ultimately they chose 6 mobile carriers – the Big Three incumbents in

---

[20] 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 carriers of significance show up in it, and that the routing patterns it reveals apply more widely.

[21] See: Obar, J.A. & Clement, A. (2013). Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty. In P. Ross and J. Shtern (eds.) TEM 2013: Proceedings of the Technology & Emerging Media Track - Annual Conference of the Canadian Communication Association (Victoria, June 5-7, 2012). Available at SSRN: http://ssrn.com/abstract=2311792 or http://dx.doi.org/10.2139/ssrn.2311792

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

Canada (Bell, Rogers and Telus), all of which we included in the 2013 report, along with their respective smaller subsidiary 'fighting' brands (Virgin Mobile, Fido and Koodo) that offer discount services to compete with independent carriers. These weren't in our 2013 sample, so we added them this year.[23]

As mentioned above, in a complementary approach to promoting greater transparency by carriers, Christopher Parsons, sent a detailed questionnaire to 18 telecom service providers focused on their handling of law enforcement requests.[24] These included 7 not in our 2013 sample[25] – Fido, included in the CILP study, and Acanac, ACN Canada, Cogeco, Sasktel, Wind Mobile, and Xplornet, which we have now included in this year's study.

Based on Parsons' work, Andrew Hilts, also of the Citizen Lab, developed an on-line tool to make it easy for individuals to exercise their rights under PIPEDA's Principle 9 – Access to information, The Access My Information (AMI) tool provided a template of an official letter requesting their carriers to provide a copy of the personal information held on them. The AMI tool, posted to the Openmedia.ca website,[26] contained carrier address information so that once someone entered the name of their carrier, along with a few other key data items, AMI would produce a correctly addressed and formatted letter that could be (e)mailed directly. Of the 26 carriers included in AMI, we added the 9 not already included in the other lists - Bruce Telecom, Comwave, Execulink, Fongo, Mobilicity, Northwestel, Novus, Telebec, VIF Internet to our 2014 sample.

Finally, Storm Internet Service, while not appearing in any of these three transparency initiatives, showed up relatively prominently in the IXmaps domestic routings data (ranked 12) so we added to our sample, bringing the total to 43 carriers.

These 19, generally small, carriers added to our study all offer retail telecom services directly to Canadian consumers. Combined with those from the 2013 report brings the total number of retail carriers assessed to 30. Their star ratings are spread across Tables 1 and 2 – Major and Minor Retailers.[27]

Awarding Stars to ISPs

Carriers earn 'stars' for each of the following **10** criteria. 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 online privacy pages are where users would look first (and likely not look further), we confined our attention to these public

---

[23] The 3+3 Project: Evaluating Canada's Wireless Carriers' Data Privacy Transparency, 2014-2015 Centre for Innovation Law and Policy Volunteer Student Working Group, Centre for Innovation Law and Policy (CILP), Faculty of Law, University of Toronto, March 12, 2015. http://innovationlaw.org/3_plus_3

[24] See Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/

[25] An eighth carrier in Parsons study not in ours, Bragg Communications, we rated under its Eastlink name.

[26] https://openmedia.ca/myinfo

[27] The distinction between Major and minor is not clean cut.

sections.[28] In an attempt to encourage carriers to ensure that privacy sections of corporate websites are comprehensive, our analysis focuses only of privacy policies (summaries and complete policies), codes of fair information practice, transparency reports, third party access guidelines/handbooks, and any other privacy-related material located in the privacy section of corporate websites. Terms of service agreements, user agreements, and all other legal materials were not assessed.

We provided all ISPs evaluated with the opportunity to respond to a preliminary version of the evaluation criteria and our initial data privacy transparency assessment of their organization. For those carriers that responded to our emails, 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.

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 the criteria the 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[29] and concerns about the 'boomerang' routing of Canadian domestic internet traffic through the US in particular[30] (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,* passed in October 2014, and *Bill C-51 – the Anti-Terrorism Act 2015,* now being hotly contested.[31]

We updated the criteria from our 2013 study in collaboration with the CILP Volunteer Student Working Group mentioned above. The CILP group greatly helped refine the 10 criteria, formulating explicit grounds for distinguishing between full, half and no stars, and prepared a much more in depth assessment of their "3 + 3" sample than ours of 43 carriers.[32]

In parallel with this collaboration, we contacted the carriers to invite their participation in formulating the criteria. We first alerted them in November to the upcoming 2014 assessment

---

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

[29] *Bill C-30 — the Protecting Children from Internet Predators Act*

[30] See: Obar, J.A. & Clement, A. (2013). Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty. In P.Ross and J. Shtern (eds.) TEM 2013: Proceedings of the Technology & Emerging Media Track - Annual Conference of the Canadian Communication Association (Victoria, June 5-7, 2012). Available at SSRN: http://ssrn.com/abstract=2311792 or http://dx.doi.org/10.2139/ssrn.2311792

[31] For C-13 see: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6311444&File=27#1; for C-51 see: http://openparliament.ca/bills/41-2/C-51/

[32] The 3+3 Project: Evaluating Canada's Wireless Carriers' Data Privacy Transparency, 2014-2015 Centre for Innovation Law and Policy Volunteer Student Working Group, Centre for Innovation Law and Policy (CILP), Faculty of Law, University of Toronto, March 12, 2015. http://innovationlaw.org/3_plus_3

exercise and solicited suggestions for refining the criteria we used in 2013. We were keen to cooperate with any carriers so interested, but while a couple of carriers replied, none made any substantive proposals. In December we posted revised draft criteria, inviting feedback. Again we received no requests for revision. On December 22, we posted the final set of criteria in the hopes that carriers would find these helpful in revising their web policies and thereby improve their scores.

The 10 criteria are as follows:[33]

1) A public commitment to PIPEDA compliance

The Personal Information Protection and Electronic Documents Act (PIPEDA), and its provincial equivalents,[34] applies to the commercial activities of all private sector organizations that exhibit a real and substantial connection to Canada, and outline rules for how they may collect, use or disclose personal information.[35] In particular, internet service providers, wireless carriers, and other telecommunications carriers, as federally regulated entities, are required to comply with PIPEDA.[36] An important requirement of PIPEDA is that personal information can only be transferred to third parties, whether Canadian or foreign, that provide an equivalent level of protection as that offered by PIPEDA. This criterion evaluates the extent to which carriers serving the Canadian market inform the public of their basic privacy responsibilities under the law.

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

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

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

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

---

[33] The criteria listed here are a slight revision of finalized criteria we posted December 22, which can be accessed at http://ixmaps.ca/documents/2014_Carrier_Evaluation_Criteria_Dec_22.pdf

[34] Provincial laws that have been deemed substantially equivalent are British Columbia's *Personal Information Protection Act*, Alberta's *Personal Information Protection Act*, and Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*. https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp The European Data Protection (1995) has also been deemed substantially equivalent.

[35] https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

[36] A single exception to this in our sample is Sasktel, which as the sole remaining provincially owned Crown Corporation telecommunications provider is covered by Saskatchewan's *Freedom of Information and Protection of Privacy Act (FOIP)* http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf

PIPEDA states that individuals have a right to be informed upon request whether their personal information has been disclosed to a third party, including the government.[37] This criteria aims to encourage carriers, in the spirit of PIPEDA's 'openness' principle to go a step further and state proactively that they will contact an individual after receiving a request for their personal information. This involves informing them it has been disclosed without the individual bearing the burden of having to first inquire.

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

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

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

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

This criteria considers whether a carrier has published information regarding the types of requests for personal data it receives and how it responds to such requests. Since 2009, a rapidly growing number of major U.S.-based internet companies regularly publish transparency reports. In 2014, for the first time, Canadian internet carriers began to follow suit. These transparency reports typically include statistics about the number of requests the companies receive from third parties, broken down by government (law enforcement, etc.), commercial and non-commercial entities. Also important is how many requests they complied with, how many accounts the requests applied to and how many disclosures of information there were. The best transparency reports mention the lawful authority that accompanied the requests (e.g. whether the request was accompanied by a warrant or other court order) and in some cases even indicate the number of secretive 'security letters' the carrier has handled.

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

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

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

[37] PIPEDA, *Principle 9 – Individual Access* https://www.priv.gc.ca/leg_c/p_principle_e.asp

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

4. Transparency about conditions for third party data disclosures.

Canadians use communication devices every day to browse the internet and transmit personal information via phone calls and text messages. The information transmitted, received, and accessed through these activities is logged by carriers who may disclose this information along with data about identity, address, and service payments to third parties. Evidence came to light in March 2014 revealing that such disclosure has been a very common occurrence, typically without carriers requiring a judicial warrant or other court order.[38] This criterion seeks to evaluate the requirements that the carrier establishes for disclosing personal information to third parties. A law enforcement handbook with this information is encouraged.

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

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

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

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

PIPEDA defines personal information broadly as "information about an identifiable person."[39] Personal information can refer to any number of variables. There have been recent controversies about whether data derived from the communication (e.g. transaction data, traffic data, userIDs or metadata more generally) or certain numbers associated with personal devices (eg IP addresses, IMSI/IMEI numbers, or MAC addresses),[40] that are enduringly associable with an individual should be regarded as 'personal information'; e.g. The Office

[38] Paul McLeod, s text to conform to the original and that used in the CILP report.f" s 44&File=27 Chronicle Herald, March 26, 2014. http://thechronicleherald.ca/novascotia/1195828-ottawa-has-been-spying-on-you. This common practice may change in light of the Supreme Court of Canada finding unanimously in *R. v. Spencer, 2014 SCC 43*, that PIPEDA prevents ISPs from disclosing customer information without finding unanimously in 1d J. Shtern (eds.) TE these critenforcement agency access to identification information, means a judicial warrant. The recently passed Bill C-13, Protecting Canadians from Online Crime Act, introduced new "lawful access" provisions facilitating such disclosure, but appear to be at odds with *Spencer* and may not be constitutional.

[39] Ibid

[40] Internet Protocol ("IP"); International Mobile Subscriber Identity ("IMSI"); International Mobile Station Equipment Identity ("IMEI"); Medium Access Control ("MAC")

of the Privacy Commissioner of Canada, has found that "An Internet Protocol (IP) address can be considered personal information if it can be associated with an identifiable individual."[41] This criterion evaluates whether a carrier has given an explicitly inclusive definition of 'personal information' in line with such best privacy practice.

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

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

No Star: The carrier gives no definition of 'personal information.'[42]

6. The normal retention periods for personal information

Companies hold on to users' personal information, including internet usage, phone calls, and GPS locations for varying lengths of time. How long they do so is a clear privacy issue and something that consumers should know. The longer personal information is kept, the more likely it is that the personal information will be exposed to misuse or disclosure.

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

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

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

[41] https://www.priv.gc.ca/leg_c/interpretations_02_e.asp#_ftn52 See also: Parsons, Christopher, "The Anatomy of Lawful Access Phone Records", posted to the "Technology, Thoughts and Trinkets" blog on 21 November 2011. https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records/

[42] We interpreted 'no definition' to include the situation of only a trivial mention that does not substantially inform a user, such as a vague term like 'internet data'.

"[Our company]shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected."[43]

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

The physical location of servers and data storage facilities is important. Data stored or processed in different jurisdictions will be subject to the associated legal regimes regardless of where the data originated or the nationality of the data subject. For instance, Canadian data stored in the United States loses the protection afforded by the Canadian Charter of Rights and Freedoms, as well as PIPEDA, and becomes subject to the USA PATRIOT Act and other surveillance authorizations.[44] In fact, Canadian data is considered under those legal authorizations to be 'foreign' to the U.S. and therefore afforded significantly reduced (little or no) safeguards compared to American data. Furthermore data storage outsourced to foreign-owned hosting services, even if physically located inside Canada, is similarly subject to foreign jurisdiction. In light of the privacy risks from the exposure of Canadians' data to foreign jurisdictions, the Office of the Privacy Commissioner found in 2008 that:

> 38. [O]rganizations that outsource the processing of personal information must provide sufficient notice with respect to the existence of service-provider arrangements, including notice that any foreign-based service provider may be required by the applicable laws of that country to disclose personal information in the custody of such service provider to the country's government or agencies.[45]

This criterion therefore evaluates whether a carrier has provided a sufficiently clear and explicit indication of possible exposure of personal information to foreign jurisdictions and what additional risks of disclosure this may entail.

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

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

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

---

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

[44] Notably the Foreign Intelligence Surveillance Act Amendments Act (2008), esp. Sec. 702, and Executive Order EO12333 (198X)

[45] https://cippic.ca/sites/default/files/OPC_Findings-canada.com.pdf

8. Transparency about where personal information is routed.

This criterion evaluates a carrier on the basis of whether or not it has indicated the relevant geographic locations or jurisdictions for routing of personal information. Data *routing*, as the particular form of information processing concerned with the switching of data packets among possible routes across the internet, affects legal privacy protection much the way that data *storage* location does, but has hitherto received comparatively little public attention. A serious concern for Canadians is that a significant proportion (>20%) of their domestic communications (i.e. communicating with other Canadian persons or services) is routed through the United States (aka "boomerang routing") and hence is subject to NSA surveillance.[46] [47] Furthermore, nearly all internet communication between Canada and third countries also passes through the U.S. or is handled by U.S. carriers, which similarly exposes it to mass suspicionless surveillance by the NSA and other state agencies.

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

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

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

9. Domestic Canadian routing when possible

This criterion evaluates whether the carrier has taken reasonable, publicly visible steps to maintain Canadian routing for domestic internet traffic. Given the additional privacy and surveillance risks facing Canadians' personal data when traveling outside Canada

---

[46] See Clement 2013. "IXmaps – Tracking your personal data through the NSA's warrantless wiretapping sites" *IEEE - ISTAS conference*, Toronto, June 26-27, 2013 https://dl.dropboxusercontent.com/u/8140293/Publications/Clement%202013%20Tracking%20your%20personal%20data%20through%20the%20NSA%E2%80%99s%20warrantless%20wiretapping%20sites%20ISTAS13%20Proceedings.pdf Obar, J.A. & Clement, A. (2013). Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty. In P.Ross and J. Shtern (eds.) TEM 2013: Proceedings of the Technology & Emerging Media Track - Annual Conference of the Canadian Communication Association (Victoria, June 5-7, 2012). Available at SSRN: http://ssrn.com/abstract=2311792 or http://dx.doi.org/10.2139/ssrn.2311792; Clement 2014. "Canada's Bad Dream" *World Policy Journal,* Special issue on "Connectivity", Fall 2014 http://www.worldpolicy.org/journal/fall2014/canada%27s-bad-dream

[47] Given that the Communication Security Establishment Canada (CSE), a close signals intelligence partner of the NSA, likely conducts similar forms of internet interception, means that keeping data exclusively in Canada does not avoid mass state surveillance, but since data that remains within Canadian jurisdiction enjoys significantly greater Constitutional and legal protection than outside, exposure to U.S. agencies adds a significant privacy risk.

or carried by foreign companies, there are good privacy reasons for routing this data within Canadian jurisdiction when possible.[48] . It clearly indicates the geo-data within Canadian jurisdiction when possible.[49] One good way is for carriers to make contracts for the handling of their domestic traffic only with Canadian internet transit providers that they can connect with in Canada and that maintain a similar policy of domestic routing when possible. Another, more publicly visible way for carriers to help ensure all-Canadian routing, is to exchange traffic or 'peer' openly at Canadian public internet exchanges points (IXPs), such as TorIX (Toronto Internet Exchange) and OttIX (Ottawa Internet Exchange) and other more recently established ones in Calgary, Winnipeg, Montreal and Halifax.

Full Star: The carrier clearly states on its privacy pages a policy of domestic Canadian routing when possible, and indicates the concrete measures it takes to achieve this goal. A carrier that verifiably peers openly at one of the Canadian IXPs will also receive a full star. Only Canadian carriers are eligible for a full star, as foreign carriers by definition subject the data they carry to non-Canadian jurisdictions.[50]

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

No Star: The carrier gives no indication of any policy or concrete measures to promote domestic routing when possible, nor does it peer openly at any Canadian public IXPs.

10. Open advocacy for user privacy rights.

This criterion is evaluated on the basis of whether or not the carrier has made clear on its privacy pages its recent (in the last five years) political, legal and/or legislative positions regarding support for user privacy rights. A carrier can demonstrate its pro-privacy position in any of the following areas:

- Public debates over mass state surveillance;
- Privacy or surveillance related legislative initiatives (e.g. the current Bill C-13 on lawful access);
- Defending user privacy rights in court; or
- Ties to advocacy organizations or initiatives promoting user privacy rights.

---

[48] 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.
[49] 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.
[50] This wording reflects a small relaxation from the original criterion, by not insisting on peering at every IXP in the service region. This may be re-visited in next yet year's study.

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

Half Star: The carrier has defended user privacy rights politically, in court or legislatively, but there is no reference to this in their privacy pages.

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

Findings

Most carriers perform very poorly on privacy transparency

As can be seen in the Star Tables, we award very few stars overall, 92.5 in total out of a possible 430. On average this is barely 2 stars out of a maximum of 10. Just 7 of the 43 carriers earned more than 3 stars, the highest being Teksavvy, with 6 stars, up from 3.5 last year. Next highest was Telus, at 5, up from 2 stars in 2013. There is much room for improvement for the carriers of Canadian's internet data.

In four criteria, no carrier received a full star

While in each of the 10 criteria at least four carriers received a half star, for these four criteria, we weren't able to award a full star to a single carrier:

#2 - A public commitment to inform users of all third party data requests
#6 - The normal retention periods for personal information
#7 - Transparency about where personal information is stored and/or processed
#8 - Transparency about where personal information is routed.

No proactive commitment to inform users of third party data requests

Just under half of the carriers in our sample (20/43) publicly state that they will inform subscribers of third party data access requests, but subscribers have to they ask first. This is the minimum legal requirement under PIPEDA.[51] No carrier yet has indicated that it will relieve their users of this significant burden and inform them proactively, as called for in **Criterion #2 - A public commitment to inform users of all third party data requests**.

Lack of indication of how long personal data is retained

Only 6 carriers go beyond the minimum PIPEDA requirement of declaring that it "*retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected,"* which is so basic that it earns no credit. None give a fulsome list of the various forms of personal data they hold, along with specific normal retention periods as required for **Criterion #6.**

Lack of transparency over where personal data is stored, processed or routed

Only about half the carriers give an indication that data may be stored in jurisdictions outside of Canada, but none go further to earn a full star for **Criterion #7** by stating what those jurisdictions are and what sort of disclosure such data may be subject. Far fewer carriers, just 4/43 give an indication of the geographical locations or jurisdictions where personal data is routed, and none meet the requirements for a full star in **Criterion #8**.

[51] For this they will receive a half star, a relaxation of the criterion from last year to help distinguish carriers that at least go this far, from the others that give their users no indication that they are entitled to this important information.

The 'fighting brands' of major mobile carriers are significantly less transparent than their corporate owners

The Big Three incumbent telecom companies in Canada that offer mobile telephony service (Bell, Rogers and Telus) all own smaller 'fighting' brands (Virgin Mobile, Fido and Koodo respectively) that offer discount services to compete with independent carriers. One would expect these subsidiaries, which operate over the same physical infrastructure, would follow similar privacy policies as their parents, but this appears not to be the case. As shown in this table, the 'fighting' brand in each case is much less transparent than its parent, as well as being below the average for the sample as a whole .

Parent	Stars		Fighting brand
Bell	3	1½	Virgin Mobile
Rogers	4	1½	Fido
Telus	5	1	Koodo

The companion "3+3" study by the CILP Volunteer Student team provides a great deal more detail about how these 6 carriers compare in terms of transparency.[52]

Canadian internet carriers have begun issuing Transparency Reports

For the first time, Canadian carriers have begun to follow the lead of major U.S. internet service providers by systematically providing statistics and other relevant details on law enforcement requests for personal data. Rogers, Sasktel, Telus, Teksavvy, and Wind are the pioneers. Carriers are also being more publically explicit about what they require from law enforcement when making such requests for personal subscriber information.

Two major U.S. Carriers scored better than most Canadian ones

The highest scoring non-Canadian carrier, AT&T, received 4 stars, placing it third highest. Another well-known US carrier that provides transit for domestic Canadian internet traffic through the US, Comcast also scored relatively well. While only garnering 2.5 stars, this placed it ahead of more than half of the 29 Canadian carriers. In neither case did these carriers indicate compliance with PIPEDA (Criterion #1), but scored better in terms of Criterion 3 Transparency about frequency of third party requests and disclosures and Criterion 4 - Transparency about conditions for third party data disclosures.

TekSavvy scores highest

In addition to receiving more stars in aggregate than any other carrier (6), TekSavvy stands out from the others by earning stars in more criteria (8) than any other. Significantly contributing

[52] The 3+3 Project: Evaluating Canada's Wireless Carriers' Data Privacy Transparency, 2014-2015 Centre for Innovation Law and Policy Volunteer Student Working Group, Centre for Innovation Law and Policy (CILP), Faculty of Law, University of Toronto, March 12, 2015. http://innovationlaw.org/3_plus_3

to TekSavvy's high score is its fulsome response to the questions that Dr. Christopher Parsons asked of 18 carriers about their handling of lawful access requests.[53]

Transit providers don't indicate explicit compliance with Canadian privacy law.

This is concerning because these behind the scenes internet carriers handle large quantities of intra-Canadian traffic, including nearly all Canadian boomerang traffic while passing through the U.S.

Transit providers scored worse than retail carriers

The 14 major transit providers that carry the bulk of long distance internet traffic (See Table 3), earned on average 1.32 stars, significantly lower than the 29 retail providers (See Tables 1 and 2), which averaged 2.4 stars. Apart from AT&T and Comcast mentioned above, the average score for transit carriers was just one star, and none earned more than 2 out of 10. Again, this lack of transparency is concerning because of the large volume of this traffic and its exposure of Canadian traffic to U.S. jurisdiction.

Cogent Communications, a U.S. transit provider and one of the largest in the world, is of particular concern since it doesn't even have a privacy policy and 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.*

This is especially significant since Cogent is ranked #3 in the IXmaps traceroute data, after Bell and Rogers, in terms of handling Canadian domestic traffic both within and outside of Canada.

Transit providers expose Canadians' traffic to risk of NSA surveillance

Since most of the transit providers carry traffic through the U.S., or otherwise bring it under U.S. jurisdiction, this exposes Canadians' data to mass state surveillance by the National Security Agency. This is concerning because when outside Canada, or handled by carriers subject to US or other jurisdictions, Canadians' data enjoy no effective legal protection, and certainly much less than when within Canadian jurisdiction.[54] [55]

---

[53] Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/

[54] Lisa M. Austin, Heather Black, Michael Geist, Avner Levin and Ian Kerr, Our data, our laws, *National Post*, December 12, 2013. http://news.nationalpost.com/2013/12/12/our-data-our-laws/
Lisa M. Austin, Enough About Me: Why Privacy is About Power, Not Consent (or Harm) Forthcoming in Austin Sarat, ed., *A World Without Privacy?: What Can/Should Law Do* (Cambridge 2014) http://ssrn.com/abstract=2524512
Lisa M Austin and Daniel Carens-Nedelsky, Jurisdiction still matters: The Legal Contexts of Extra-National Outsourcing, presented at the Assessing Privacy Risks of Extra-National Outsourcing of eCommunications public forum, *Seeing Through the Cloud: Why Jurisdiction Still Matters in a Digitally Interconnected World*, University of Toronto, March 6, 2015. See webcast at: http://mediacast.ic.utoronto.ca/20150306-eComm/index.htm

[55] 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

Given the lack of equivalent privacy protection between Canada and the U.S., the many Canadian retail internet carriers that rely on U.S. transit providers or U.S. routing for Canadian domestic internet traffic (aka 'boomerang' routing) calls into question whether they are complying with their PIPEDA obligations to only transfer personal information to third parties that offer an equivalent level of privacy protection.

Privacy and transparency material are often scattered and disorganized

Many of the privacy sections of the corporate websites assessed were poorly organized, messy and inconsistent. Privacy documents are already notoriously difficult to read and understand. Yet, while some carriers did present an organized page with clearly labeled links to a privacy policy, and in some instances a transparency report and/or code of fair information practices, many failed to link all relevant documents to a comprehensive privacy section. For some, the "privacy" link on the main corporate page didn't link to a general privacy policy, but rather to a privacy policy for their website. In other cases, privacy policies were inconsistent, presenting conflicting material in related documents. Very few carriers assessed demonstrated the level of sophisticated presentation in their policies reflected in the rest of their website.

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.

Recommendations

Without proactive public reporting on the part of carriers 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 carriers that handle Canadian internet traffic.
Carriers 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 carriers 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 their legal obligation to ensure that 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 proactively when personal data has been requested by a third party

All carriers that handle Canadian internet traffic should prominently display a public 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 carriers 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, carriers 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 carriers 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 carriers 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 carriers 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 carriers 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 carriers 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 carriers 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 carriers 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 carriers 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: How they advocate for their subscribers' privacy rights.

All carriers that handle Canadian internet traffic should clearly indicate their current stance on personal data privacy protection and mass state surveillance. This stance should include their position on alleged NSA and CSE surveillance of Canadian internet transmissions. If a carrier 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. A carrier should be similarly transparent if it is involved in any court case around the privacy rights of their subscribers. Whatever the carrier's position in relation to user privacy rights, this should be made publicly clear.

Recommendation 11: Consolidate all privacy and transparency policy information so it is easily accessible though the main corporate privacy page.

"Privacy" or "Privacy Policy" links should be prominently displayed in an easy-to-find position on the corporate website. The privacy link should connect to a comprehensive privacy section of the website that includes all privacy and transparency materials. Users should not have to conduct Google searches to find transparency reports and other relevant documents. All privacy materials should be up-to-date and language should be consistent across all documents.

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

Recommendation 12: 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 carriers 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 carriers only hand off internet traffic to carriers that meet Canadian privacy law standards.

Recommendation for legislators and politicians.

Recommendation 13: 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 14: 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 15: Canadian law enforcement and security agencies should proactively publish statistics about requests for personal information they make to carriers

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, carrier responses, and how these have assisted or not in achieving their mandates.

This report calls on carriers, 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 carriers 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. They will also earn the trust of Canadians who rely on them for the safe handling of their personal and sensitive data.

Appendix: Carrier Profiles and Evaluations

Following are the details of our evaluations for each of the 43 internet carriers in our selected sample of leading telecommunications carriers providing intra-Canadian internet carrier services. Each entry includes the following:

- **Carrier name**,
- The location of corporate **headquarters**,
- **Parent company,**
- The **nationality** of the carrier indicating possible non-Canadian jurisdictional accountability,
- 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 carriers from routing data,
- **AS rank, as reported by CAIDA** – The Cooperative Association for Internet Data Analysis in late 2014. CAIDA's ASN rankings are based on the number of IPv4 addresses within the AS, and give an indication of the relative size of a carrier in terms of its routing connections and capacity globally, See: http://as-rank.caida.org/
- **AS rank, as reported by the IXmaps report**. IXmaps rankings give a rough indication of the relative importance of the carriers in this sample in terms of the number of routing hops involved in routing Canadian domestic internet traffic, as captured in the IXmaps database of approximately 9500 non-duplicated intra-Canadian traceroutes, See: http://ixmaps.ca/as-rank
- A brief **description** of the carrier,
- A table showing 'star' ratings for each of the 10 criteria, with explanatory notes,
- The primary sources for **Privacy, Transparency** and **Third Party Access Guideline** materials where available, as well as the date of latest revision,
- **Explanatory notes,**
- **Presence at Canadian Public Internet Exchange Points (IXPs):**
    - TorIX- Toronto http://www.torix.ca/peers,
    - OttIX - Ottawa http://www.ottix.net/
    - YYCIX – Calgary http://yycix.ca/peers.html
    - **Appearance in other privacy transparency reporting initiatives:**
    - IXmaps 2013 Report
    - Citizen Lab/Chris Parsons[1]
    - Digital Stewards Initiative/ Access My Information (AMI) tool[2]
    - Centre for Innovation Law and Policy (CILP)[3]

---

[1] See Christopher Parsons (2014), Towards Transparency in Canadian Telecommunications, blog post, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/

[2] https://openmedia.ca/myinfo

[3] The 3+3 Project: Evaluating Canada's Wireless Carriers' Data Privacy Transparency, 2014-2015 Centre for Innovation Law and Policy Volunteer Student Working Group, Centre for Innovation Law

AboveNet Communications (Zayo)

Headquarters: White Plains, NY, U.S.A.
Corporate parent: Zayo Group
Nationality: U.S.A.
Corporate site: http://www.above.net

ASN (s): 6461, 17025
CAIDA AS Rank: 19
IXmaps AS rank: 15

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."[4] 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, co-location, and IP services".[5]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**0**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored and/or processed	0	**0**	
8) Transparency about where personal information is routed.	0	**½**	[1]
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:

---

and Policy (CILP), Faculty of Law, University of Toronto, March 12, 2015. http://innovationlaw.org/3_plus_3

[4] http://www.above.net/products/metroenet.php

[5] http://www.zayo.com/abovenet

Primary Privacy page: http://www.above.net/corporate/disclaimer.php# (Last revised: 2012)
Transparency Report (URL): Not found
Third Party Access Guidelines/Handbook: Not found

Notes:
[1] Provides a very detailed interactive network map of fibre routes and facilities, but doesn't provide any specific consumer oriented information about where personal information may be routed.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	Yes

Acanac

Headquarters: Mississauga, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.acanac.ca/

ASN (s): 33139
CAIDA AS Rank: 5981
IXmaps AS rank: 28

Acanac is a privately owned Canadian ISP serving primarily Ontario and Quebec. It has roughly 70,000 clients in Canada and serves both homes and businesses.[6] Acanac offers TV, phone, and Internet service to their customers.

Evaluation Criteria	Stars 2013	**Stars 2014**	[1]
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**0**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page http://www.acanac.ca/PRIVACY-POLICY.html (Last revised: 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:
[1] The privacy policy appears to refer only to their website. Acanac has some material on data disclosure buried in their Terms of Service agreement, but this material does not

[6] http://www.acanac.ca/Company-Info.html

appear in the privacy policy. It should be added that their Terms of Service agreement is very messy and poorly organized.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

ACN Canada

Headquarters: Montreal, Que, Canada
Corporate parent: ACN Inc.
Nationality: U.S.A.
Corporate site: http://acncanada.ca/

ASN (s): 17899
CAIDA AS Rank: 6964
IXmaps AS rank: 29+

ACN Canada is a subsidiary of its parent ACN Inc., which began providing resold long distance services, and gradually expanded into other telecommunications services. ACN was founded in 1993 and expanded to Canada in 1997, where it offers phone and Internet services. ACN has since expanded to 24 countries, including Australia, The Netherlands, South Korea, and Poland[7].

Evaluation Criteria	Stars 2013	**Stars 2014**	[1]
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.myacncanada.ca/privacy.html (Last revised: Unclear)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[7] http://acncanada.ca/company

[1] A Google search for ACN Canada brings up http://acncanada.ca/. The privacy policy on this site is not Canadian-specific, it appears to be their international privacy policy. Further Google searching reveals a second site: http://www.myacncanada.ca/ that has a Canada-specific privacy policy. Only the Canadian policy was evaluated for this study. It is recommended that ACN make it easier for Canadians to find their correct website and privacy policy.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

American Telephone and Telegraph (AT&T)

Headquarters: Dallas TX, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site: https://www.att.com/

ASN (s): 7018, 17227, 7132
CAIDA AS Rank: 12
IXmaps AS rank: 27

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"[8].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	½	**1**	[1]
4) Transparency about conditions for third party data disclosures.	½	**1**	[2]
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**1**	[3]

Primary Sources:

[8] http://www.att.com/gen/investor-relations

Primary Privacy page: http://www.att.com/gen/privacy-policy?pid=2506 (Last revised: 2015) (Secondary Privacy page(s): https://www.att.com/gen/privacy-policy?pid=13692)
Transparency Report: http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (Last revised: 2015)
Third Party Access Guidelines/Handbook: Not Found

Notes:
[1] Detailed transparency report, but US focused
[2] As part of their transparency report, they include information describing what constitutes: national security demands, U.S. criminal and civil demands, location demands, international demands and emergency requests. For example: http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html
[3] Includes a section called "Privacy Advocacy" in their transparency report.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Not accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Bell Canada

Headquarters: Verdun, Quebec, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.bell.ca/

ASN (s): 577, 6549, 11489
CAIDA AS Rank: 81
IXmaps AS rank: 1

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.[9]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy#displayStep Last revised: 2015) (Secondary Privacy page(s): http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy#displayStep)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[9] http://www.bce.ca/aboutbce/bellcanada/residentialservices/

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	Invited

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	Yes

Bell Aliant

Headquarters: Verdun, Quebec, Canada
Corporate parent: Bell Canada Enterprises
Nationality: Canada
Corporate site: http://www.bellaliant.net/

ASN (s): 855
CAIDA AS Rank: 504
IXmaps AS rank: 10

Bell Aliant is a Canadian telecommunications provider, serving Canadians throughout Atlantic Canada and in select regional markets in Ontario and Quebec[10]. Bell Aliant was created in 1999[11] "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."[12] Bell Aliant offers telephone, "data, Internet, video and value-added business solutions"[13].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.bellaliant.net/privacy-security (Last revised: 2015)

[10] "Bell Aliant: Regions We Serve," accessed May 24, 2013, http://bellaliant.ca/english/about/regions.shtml.
[11] "Bell Aliant Timeline," accessed May 24, 2013, http://www.bellaliant.ca/english/about/popup_timeline8.html.
[12] "About Bell Aliant," accessed May 24, 2013, http://bellaliant.ca/english/about/index.shtml.
[13] "Bell Aliant News," accessed May 24, 2013, http://bell.aliant.ca/english/news/view_art.asp?id=2217.

Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

Bruce Telecom

Headquarters: Bruce Country, ON, Canada
Corporate parent: Municipality of Kincardine
Nationality: Canada
Corporate site:
http://www.brucetelecom.com/

ASN (s): 11727
CAIDA AS Rank: 8502

IXmaps AS rank: 29+

Bruce Telecom is a 100 Year-old corporation owned by the Municipality of Kincardine, which operates in Kincardine, Port Elgin, Tiverton, Southampton, Owen Sound and surrounding areas[14]. It offers telephone, mobile, and DSL internet service to these areas.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	½	
2) A public commitment to inform users of all third party data requests	-	½	[1]
3) Transparency about frequency of third party requests and disclosures	-	-	
4) Transparency about conditions for third party data disclosures.	-	½	
5) An explicitly inclusive definition of 'personal information'.	-	-	
6) The normal retention periods for personal information	-	½	
7) Transparency about where personal information is stored/processed	-	-	
8) Transparency about where personal information is routed.	-	-	
9) Domestic Canadian routing when possible	-	-	
10) Open advocacy for user privacy rights	-	-	

Primary Sources:
Primary Privacy page: http://www.brucetelecom.com/governance-details.php?id=2 (Last revised: 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[14] http://www.brucetelecom.com/aboutus.php

[1] They note "Bruce Telecom may notify customers that an order has been received, if the law allows it. Notification of such orders may be done by telephone, electronic mail or by letter to the customers last known address." The word "may" requires that this remain a half-star.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Cogeco

Headquarters: Montreal, QC, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.cogeco.ca

ASN (s): 7992
CAIDA AS Rank: 378
IXmaps AS rank: 25

Cogeco operates both broadband, home phone, and television service in Canada, mostly in Ontario and Quebec. In the United States it operates through its subsidiary Atlantic Broadband (http://atlanticbb.com/). Cogeco also provides data hosting services, through PEER 1 (http://www.peer1.ca/) and owns 13 radio stations in Quebec.[15]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**1**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.cogeco.ca/cable/corporate/cca/privacy_policy.html (Last revised: February 2012) (Secondary Privacy page(s): http://www.cogeco.ca/export/sites/cogeco/corporate/files/legal/Cogeco_Privacy_Commitment.pdf)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[15] http://www.cogeco.ca/cable/corporate/cgo/main.html

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

Cogent Communications

Headquarters: Washington DC, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site: http://www.cogentco.com

ASN (s): 174
CAIDA AS Rank: 2
IXmaps AS rank: 3

Cogent Communications is a multinational internet carrier, with subscribers in more than 36 countries and 180 markets[16]. 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"[17].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	[1]
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**0**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**½**	[2]
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.cogentco.com/en/acceptable-use-policy (Last revised: 2011)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[16] "Cogent: History," accessed May 24, 2013, http://www.cogentco.com/en/about-cogent/history.
[17] "About Cogent," accessed May 24, 2013, http://www.cogentco.com/en/about-cogent.

Notes:
[1] As in 2013, there is not privacy page, only this statement in its Acceptable Use Policy page: "Cogent makes no guarantee of confide0tiality 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] Provides a network map of fibre routes and facilities, but doesn't provide any specific consumer oriented information about where (esp. jurisdictions) personal information may be routed.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Comcast

Headquarters: Philadelphia, PA, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site:
https://www.comcast.com/

ASN (s): 7922
CAIDA AS Rank: 28
IXmaps AS rank: 22

Comcast was created as an independent company in 1963[18]. Comcast offers home television and Internet service. As part of their recent merger with NBC Universal they are now involved in a host of media related services.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**½**	
4) Transparency about conditions for third party data disclosures.	-	**1**	[1]
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**½**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.comcast.com/corporate/legal/privacyStatement.html (Last revised: January 13, 2014) (Secondary Privacy page(s): https://www.comcast.com/Corporate/Customers/Policies/CustomerPrivacy.html (Last revised: August 1, 2014)
Transparency Report: http://corporate.comcast.com/comcast-voices/comcast-issues-first-transparency-report (Last revised: March 20, 2014)
Third Party Access Guidelines/Handbook:
http://cdn.comcast.com/~/Media/Files/Legal/Law%20Enforcement%20Handbook/Comc

[18] http://corporate.comcast.com

ast%20Xfinity%202012%20Law%20Enforcement%20Handbook%20v022112.pdf?vs=1
(Last revised: February 2012)

Notes:
[1] Have detailed Law Enforcement Access Handbook.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Comwave

Headquarters: Toronto, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site:
http://www.comwave.net/

ASN (s): 15128
CAIDA AS Rank: 5930
IXmaps AS rank: 29+

Comwave is an independently owned company that specializes in VOIP across Canada. They provide internet services as well[19].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.comwave.net/legals/ (Last revised: 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**

[19] http://www.comwave.net/about/

Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Distributel

Headquarters: Ottawa, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site:
https://www.distributel.ca/

ASN (s): 11814, 14595
CAIDA AS Rank: 6462
IXmaps AS rank: 20

Distributel Communications is an Ottawa, ON based[20] company offering high speed Internet services, telephone services and long distance plans to residents of British Columbia, Alberta, Ontario, and Quebec.[21] Distributel began in 1988, as "one of the pioneers of the competitive long-distance industry in Canada"[22].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**½**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**0**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	1	**1**	
10) Open advocacy for user privacy rights	½	**0**	

Primary Sources:
Primary Privacy page: http://www.distributel.ca/en/privacy.aspx (Undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[20] "Contact Us | Distributel," *Distributel.ca*, accessed May 24, 2013, http://www.distributel.ca/en/contact.aspx.
[21] "About Us | Distributel," *Distributel.ca*, accessed May 24, 2013, http://www.distributel.ca/en/aboutus.aspx.
[22] Ibid.

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

Eastlink

Headquarters: Halifax, NS
Corporate parent: -
Nationality: Canada
Corporate site: http://www.eastlink.ca/

ASN (s): 11260
CAIDA AS Rank: 468
IXmaps AS rank: 14

Eastlink provides telecommunications, entertainment, and advertising services to residents of "Atlantic Canada, Ontario, Quebec, Alberta, Manitoba, British Columbia and Bermuda"[23]. 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[24], Halifax, Nova Scotia-based Eastlink is the "the largest, privately held telecommunications company in the country and the fifth largest teleco overall in Canada"[25].

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.eastlink.ca/portals/0/about/customer_privacy_policy-eastlink.pdf (Last revised: January 2015) (Secondary Privacy page(s):

[23] http://www.eastlink.ca/About.aspx.
[24] http://www.manta.com/ic/mt6l1qn/ca/bragg-communications-incorporated.
[25] http://www.eastlink.ca/About/History.aspx.

http://www.eastlink.ca/portals/0/about/eastlinkconsumertermsofservice.pdf (Last revised: December 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	Yes	-

Execulink

Headquarters: Kitchener, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.execulink.ca/

ASN (s): -
CAIDA AS Rank: -
IXmaps AS rank: 29+

Execulink is a telecom provider in South-western Ontario, and provides Internet, television, phone and mobile services. Execulink has a strong focus on creating personal relationships with their customers and giving back to their community. It also supports several free Wi-Fi hotspots in towns in South-western Ontario.[26]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**1**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page:
http://www.execulink.ca/files/1114/1631/6465/PRIVACY_POLICY_v3.pdf (Last revised: July 28, 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[26] http://www.execulink.ca/about-us/

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Fido

Headquarters: Montreal, Que, Canada
Corporate parent: Rogers
Nationality: Canada
Corporate site: http://www.fido.ca/

ASN (s): 8282
CAIDA AS Rank: 3910
IXmaps AS rank: 29+

In 1996 Microcell Solutions Inc. launched Fido. Fido now offers voice and data plans as one of the 'fighting brands' of Rogers. It offers GSM, 4G HSPA+ and LTE networks across most of Canada, and have 300 partners worldwide to provide their customers with global coverage.[27]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**½**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page:
http://www.fido.ca/web/content/terms/privacy_policy?lang=en&cm_mmc=Redirects-_-External-_-Marketing-_-privacypolicy (Last revised: 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[27] http://www.fido.ca/web/content/aboutus#network

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	Yes

Fongo

Headquarters: Waterloo, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.fongo.com/

ASN (s): -
CAIDA AS Rank: -
IXmaps AS rank: 29+

Fongo is a VoIP service for mobile phones, which allows users to maintain their current plan with another provider. For example one could have a phone plan with a major telecom in the Toronto area and then use a Fongo VOIP number to avoid having to make long distance calls if they were in the Ottawa area.[28]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**½**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.fongo.com/legal/privacy/ (Undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

[28] http://www.fongo.com/how-it-works/

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Hurricane Electric Internet Services

Headquarters: Fremont, CA, U.S.A
Corporate parent: -
Nationality: U.S.A
Corporate site: https://www.he.net/

ASN (s): 6939
CAIDA AS Rank: 9
IXmaps AS rank: 11

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."[29] It is 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 Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	½	**½**	
9) Domestic Canadian routing when possible	1	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: https://www.he.net/privacy.html (Undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[29] http://www.he.net/about_us.html

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	Open

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Koodo Mobile

Headquarters: Vancouver, BC, Canada
Corporate parent: Telus
Nationality: Canada
Corporate site: http://koodomobile.com/

ASN (s): -
CAIDA AS Rank: -
IXmaps AS rank: 29+

Koodo Mobile is a subsidiary of Telus. Its main selling point is their Canada-wide calling plans. Koodo offers 'tab' based plans that allow customers to pay off their phones over the course of their contract, rather than having the phone be subsidized by the contract.[30]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://koodomobile.com/en/on/legal.shtml (Undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

[30] http://koodomobile.com/en/on/about.shtml

TorIX- Toronto	OttIX - Ottawa	YYCIX - Calgary
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	Yes

Level 3 Communications

Headquarters: Broomfield, CO, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site: www.level3.com

ASN (s): 3356, 3549, 30686
CAIDA AS Rank: 1
IXmaps AS rank: 13

Level 3, a Colorado-based telecommunications company, claims to be one of the "world's top three Internet traffic carriers,"[31] and one of only six Tier 1 Internet providers globally.[32] 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.[33]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.level3.com/en/privacy/ (Last revised: January 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[31] http://www.level3.com/en/about-us/company-information/company-history/
[32] http://www.level3.com/en/about-us/
[33] http://www.level3.com/~/media/Assets/fact_sheets/fact_sheet_canada.ashx

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Limelight

Headquarters: Tempe, AZ, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site:
http://www.limelight.com/

ASN (s): 22822, 45396, 38622
CAIDA AS Rank: 202
IXmaps AS rank: 17

Limelight's focus is on quick content delivery for its customers, mostly being medium to large companies needing to reach a global audience. It specializes in networks meant to deliver media, cloud storage or software, gaming, and other high bandwidth applications.[34] Many of their services are offered through their Limelight Orchestrate Platform, which is designed allow users to customize their experience and maintain control over their content as they distribute it.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.limelight.com/company/privacy-policy/ (Last revised: 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[34] http://www.limelight.com/company/we-help-you/

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Mobilicity

Headquarters: Vaughan, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://mobilicity.ca/

ASN (s): 36676
CAIDA AS Rank: 8721
IXmaps AS rank: 29+

Mobilicity is an independent mobile carrier offering several zones of coverage in Canada, including Toronto, Ottawa, Calgary, Edmonton and Vancouver.[35]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://mobilicity.ca/media/files/documents/Privacy_Policy_2.pdf (Undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**

[35] http://mobilicity.ca/how-we-are-different/

-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

MTS Allstream

Headquarters: Winnipeg, MB, Canada
Corporate parent: -
Nationality: Canada
Corporate site:
http://www.mtsallstream.com/

ASN (s): 15290, 7122
CAIDA AS Rank: 136
IXmaps AS rank: 29+

MTS Allstream is a Winnipeg, Manitoba-based telecommunications company delivering high speed Internet, wireless, digital TV, converged IP networking, and residential telephone services.[36] 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.[37] The company is the fourth-largest communications provider in Canada.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	½	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.mtsallstream.com/legal/ (Last revised: 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[36] "Corporate Profile | MTS," accessed May 24, 2013, http://www.mts.ca/mts/about+mts+allstream/our+company/corporate+profile.
[37] "Our Business | MTS," accessed May 24, 2013, http://www.mts.ca/mts/about+mts+allstream/our+company/our+business.

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional[38]	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

[38] Note: Is referred to as Allstream, not MTS Allstream

NorthwesTel

Headquarters: Whitehorse, Yukon, Canada
Corporate parent: Bell[39]
Nationality: Canada
Corporate site: http://www.nwtel.ca/

ASN (s): 22573, 6058
CAIDA AS Rank: 2791
IXmaps AS rank: 26

NorthwesTel operates in Northern Canada as a subsidiary of Bell. NorthwesTel is the sole supplier of telecommunications north of the 60th parallel. It offers a variety of services including Internet, home phone, mobile phone and television. It has been owned by Bell Canada Enterprises since 1988.[40]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.nwtel.ca/northwestel-policies/northwestel-privacy-policy-and-code (Last revised: 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[39] http://www.crtc.gc.ca/ownership/eng/cht143c.pdf
[40] http://www.nwtel.ca/about-northwestel/history-first-in-the-north

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Novus

Headquarters: Vancouver, BC, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.novusnow.ca/

ASN (s): 40029
CAIDA AS Rank: 5113
IXmaps AS rank: 29

Novus positions itself as an alternative to the major providers in Vancouver and the surrounding area. Most of its operations are in British Columbia, where they offer Internet, television and home phone services.[41]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**½**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.novusnow.ca/privacy-policy/ (Last revised: February 18, 2015)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

[41] http://www.novusnow.ca/about-novus/

TorIX- Toronto	OttIX - Ottawa	YYCIX - Calgary
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Peer 1 Hosting

Headquarters: Vancouver, BC
Corporate parent: Cogeco[42]
Nationality: Canda
Corporate site: http://www.peer1.ca/

ASN (s): 13768
CAIDA AS Rank: 144
IXmaps AS rank: 6

PEER 1 Hosting is a global web hosting company, specializing in "Managed Hosting, Dedicated Hosting, Colocation, Cloud Hosting and Network Services."[43] Launched in 1999 and based in Vancouver, British Columbia, PEER 1 is now a subsidiary of Cogeco Cable.[44] PEER 1 offers 20 state-of-the-art datacenters and 10 colocation facilities across Europe and North America.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**0**	
5) An explicitly inclusive definition of 'personal information'.	½	**0**	
6) The normal retention periods for personal information	½	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.peer1.ca/about-us/legal/privacy-policy (Last revised: August 7, 2013)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[42] http://www.cogeco.ca/cable/corporate/cca/main.html
[43] "PEER 1 Hosting Fact Sheet | PEER 1 Hosting," accessed May 24, 2013, http://www.peer1.ca/why-peer-1/peer-1-hosting-fact-sheet.
[44] "PEER 1 Hosting Extends PCI Compliance Accreditation," accessed May 24, 2013, http://www.peer1.ca/news-update/peer-1-hosting-extends-pci-compliance-accreditation.

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Primus Telecommunications (Canada)

Headquarters: Toronto, ON
Corporate parent: Primus Telecommunications Group[45]
Nationality: United States of America
Corporate site: http://primus.ca/

ASN (s): 9443, 6407
CAIDA AS Rank: 412

IXmaps AS rank: 21

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."[46]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	**½**	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**½**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	1	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://primus.ca/index.php/bc_en/privacy-policy (Last revised: 2015? - undated)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

[45] http://primus.ca/index.php/ont_en/about-us/corporate-overview
[46] http://primus.ca/ont_en/about-us

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	Peering	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

Rogers Communications

Headquarters: Toronto, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.rogers.com/

ASN (s): 812, 3602
CAIDA AS Rank: 153
IXmaps AS rank: 2

Rogers Communications is "Canada's largest provider of wireless voice and data communications services."[47] Rogers provides cable television, high speed Internet, residential telephone, and mobile phone services (via its three mobile phone brands, Rogers, Fido, and Chatr).[48]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**½**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**½**	[1]
4) Transparency about conditions for third party data disclosures.	0	**½**	[2]
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**½**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**1**	

Primary Sources:
Primary Privacy page: http://www.rogers.com/web/content/Privacy-Policy (Last revised: November 13, 2006)
Transparency Report: http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf (Undated)

Third Party Access Guidelines/Handbook: Not Found

[47] "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.
[48] "Get to Know Rogers - Media Kit - Rogers Newsroom."

Notes:
[1] Rogers is among the first Canadian carriers to issue a Transparency Report, which is commendable. However, it is missing several key ingredients, notably statistics on disclosures as distinct from requests as well as requests by non-governmental bodies (eg copyright holders)
[2] TP mentions various types of government request. Indicates a warrant is needed for metadata.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	Yes

Sasktel

Headquarters: Regina, SK
Corporate parent: Province of Saskatchewan[49]
Nationality: Canada
Corporate site: http://www.sasktel.com

ASN (s): 803
CAIDA AS Rank: 1269

IXmaps AS rank: 23

Sasktel is a Crown Corporation operated by the province of Saskatchewan.[50] It offers mobile phone, television, Internet and home phone services to the province. In addition to these services Sasktel offers home security through their SecurTek brand.[51]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**½**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**½**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:

[49] http://www.cicorp.sk.ca/crown_corporations/sasktel

[50] As a Crown Corporation, it is one of the few telecom services providers in Canada that does not operate under the provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA), but in this case Saskatchewan's *Freedom of Information and Protection of Privacy Act (FOIP)* http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf

[51] http://www.sasktel.com/wps/wcm/connect/content/home/about-sasktel/

Primary Privacy page: http://www.sasktel.com/wps/wcm/connect/content/home/about-sasktel/legal-and-regulatory/privacy-policy/privacy-policy (Last revised: November 2013)
Transparency Report: http://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES (Undated)
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

Savvis Communications (CenturyLink)

Headquarters: St. Louis, Missouri, U.S.A.
Corporate parent: Century Link[52]
Nationality: U.S.A.
Corporate site: www.savvis.com

ASN (s): 3561, 6347, 4298
CAIDA AS Rank: 24
IXmaps AS rank: 16

Savvis provides "IT infrastructure solutions" such as "cloud, colocation and managed-hosting services"[53] 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.[54] 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."[55]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**0**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:

[52] http://www.centurylinktechnology.com/contact
[53] http://news.centurylink.com/index.php?s=43&item=3072
[54] http://www.centurylink.com/Pages/AboutUs/CompanyInformation/
[55] http://www.savvis.ca/en-ca/company/pages/history.aspx

Primary Privacy page: http://www.centurylinktechnology.com/legal/privacy-policy (Last revised: May 1, 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

Shaw Communications

Headquarters: Calgary, AB, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.shaw.ca/

ASN (s): 6327
CAIDA AS Rank: 120
IXmaps AS rank: 5

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.[56]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	½	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.shaw.ca/privacy-policy/ (Last revised: April 2, 2014)
Transparency Report: Not Found
Third Party Access Guidelines/Handbook: Not Found

Notes:

[56] "About Shaw," accessed May 24, 2013, http://www.shaw.ca/Corporate/About-Shaw/Shaw-Companies/.

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

Sprint

Headquarters: Overland Park, KS, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site: https://www.sprint.com

ASN (s): 1239, 1803, 3644
CAIDA AS Rank: 17
IXmaps AS rank: 24

Sprint offers 4G wireless coverage throughout most of the United States. It has 56 million customers and is a Fortune 100 company..[57]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**1**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: https://www.sprint.com/legal/privacy.html (Last revised: May 2, 2014) (Secondary Privacy page(s): https://www.sprint.com/legal/docs/SprintIntDataPrivacyPolicy.pdf (Last revised: November 7, 2014))
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

[57] http://newsroom.sprint.com/about-us/?ECID=vanity:about

TorIX- Toronto	OttIX - Ottawa	YYCIX - Calgary
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Storm Internet Service

Headquarters: Perth, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: https://www.storm.ca/

ASN (s): 13319
CAIDA AS Rank: 2967
IXmaps AS rank: 12

Storm Internet Service offers DSL, Cable and dial-up. It has been offering said services since 1996 across Ontario and in parts of Western Quebec.[58]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**0**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**½**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: https://www.storm.ca/terms-of-service/privacy/ (Undated)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**

[58] https://www.storm.ca/about-storm/

Conditional	Peering	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Tata Communications

Headquarters: Mumbai, Maharashtra, India
Corporate parent: -
Nationality: India
Corporate site:
http://www.tatacommunications.com/

ASN (s): 6453, 6421
CAIDA AS Rank: 7
IXmaps 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".[59]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	0	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**1**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	½	**`½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://www.tatacommunications.com/policies/privacy-policy (Undated)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

[59] http://microsites.tatacommunications.com/about/overview.asp

TorIX- Toronto	OttIX - Ottawa	YYCIX - Calgary
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

TekSavvy Solutions

Headquarters: Chatham, ON, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://teksavvy.com/

ASN (s): 5645, 20375
CAIDA AS Rank: 1022
IXmaps AS rank: 8

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.[60] Teksavvy relies on the "last mile" infrastructure of other carriers including Rogers to deliver its services.[61] Teksavvy's motto is "We're Different. In a Good Way," and the company bills itself as an alternative to the "usual corporate monopolies."[62]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	½	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**1**	
4) Transparency about conditions for third party data disclosures.	½	**1**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**½**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	1	**1**	
10) Open advocacy for user privacy rights	½	**½**	

Primary Sources:

---

[60] "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.
[61] "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/.
[62] "TekSavvy - Who We Are," accessed May 24, 2013, http://www.teksavvy.com/en/why-teksavvy/company/who-we-are.

Primary Privacy page: http://teksavvy.com/en/why-teksavvy/policies/privacy-policy (Undated)
Transparency Report: http://teksavvy.com/en/why-teksavvy/policies/legal-stuff/transparency-report (Last revised: June 4, 2014)
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	-	-

Telebec

Headquarters: Bécancour, Que, Canada
Corporate parent: Bell[63]
Nationality: Canada
Corporate site: https://www.telebec.com/

ASN (s): 35911
CAIDA AS Rank: 5957
IXmaps AS rank: 29+

Telebec is a subsidiary of Bell Canada Enterprises that provides telecommunications services, including mobile and home phone, and Internet to 150,000 customers in Quebec. Telebec's service area is southern and eastern Quebec, which includes 300 municipalities.[64]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**1**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page:
http://www.telebec.com/english/template/frame.asp?Section=general&Partie=propos_telebec&Page=infoslegales_securite.asp (Last revised: 2013) (Secondary Privacy page(s):
http://www.telebec.com/english/general/propos_telebec/pdf/policeng.pdf (Last revised: January 31, 2011)
Transparency Report: Not found

---

[63] http://www.crtc.gc.ca/ownership/eng/cht143a.pdf
[64] http://www.telebec.com/english/template/frame.asp?Section=general&Partie=propos_telebec&Page=propos_de_telebec.asp

Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

TeliaSonera

Headquarters: Stockholm, Sweden
Corporate parent: -
Nationality: Sweden
Corporate site:
https://www.teliasonera.com/

ASN (s): 1299
CAIDA AS Rank: 4
IXmaps AS rank: 18

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.[65]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	0	**0**	
2) A public commitment to inform users of all third party data requests	0	**0**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**0**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page:
http://www.teliasonera.com/Documents/Public%20policy%20documents/Privacy_Policy_Dec_2012.pdf(Undated)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

[65] http://www.teliaSonera.com/

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	-	-	-

TELUS

Headquarters: Vancouver, BC, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://www.telus.com

ASN (s): 852, 7861, 54719
CAIDA AS Rank: 146
IXmaps 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.[66]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**1**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**½**	[1]
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**½**	
7) Transparency about where personal information is stored/processed	0	**½**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	½	**1**	

Primary Sources:
Primary Privacy page: http://about.telus.com/community/english/privacy (Last revised: 2015)
Transparency Report: http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf (Undated)
Third Party Access Guidelines/Handbook: Not found

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

Notes:
[1] Telus is among the first Canadian carriers to issue a Transparency Report, which is commendable. However, it is missing several key ingredients, notably statistics on disclosures as distinct from requests as well as requests by non-governmental bodies (e.g. copyright holders).

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	Invited

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	Yes

Verizon

Headquarters: Basking Ridge, NJ, U.S.A.
Corporate parent: -
Nationality: U.S.A.
Corporate site:
https://www.verizon.com/

ASN (s): 701, 702, 703
CAIDA AS Rank: 13
IXmaps AS rank: 19

Verizon is a major ISP in the U.S.[67] The company is a global leader in delivering broadband to their consumer, government, and business customers. Global Traveller in December 2013 named them the Best Wireless Service in The World.[68]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**½**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**1**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: https://www22.verizon.com/about/privacy/policy/ (Last revised: August 2014)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found
Notes:

Presence at Canadian Public IXPs

[67] https://www.verizonwireless.com/aboutus.html
[68] https://www.verizonwireless.com/aboutus/company/awards.html

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	-	-

Vidéotron

Headquarters: Montreal, Que, Canada
Corporate parent: -
Nationality: Canada
Corporate site:
http://www.videotron.com/

ASN (s): 5769
CAIDA AS Rank: 552
IXmaps AS rank: 9

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 Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	1	**½**	
2) A public commitment to inform users of all third party data requests	0	**½**	
3) Transparency about frequency of third party requests and disclosures	0	**0**	
4) Transparency about conditions for third party data disclosures.	½	**½**	
5) An explicitly inclusive definition of 'personal information'.	0	**½**	
6) The normal retention periods for personal information	0	**0**	
7) Transparency about where personal information is stored/processed	0	**0**	
8) Transparency about where personal information is routed.	0	**0**	
9) Domestic Canadian routing when possible	0	**0**	
10) Open advocacy for user privacy rights	0	**0**	

Primary Sources:
Primary Privacy page: http://corpo.videotron.com/site/securite-confidentialite-en.jsp (Last revised: 2013) (Secondary Privacy page(s): http://corpo.videotron.com/static/site/static/pdf/en/code_videotron.pdf (Last revised: August 2, 2013)

[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.

Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
Yes	Yes	Yes	-

VIF Internet

Headquarters: Montreal, Que, Canada
Corporate parent: -
Nationality: Canada
Corporate site: http://service.vif.com/

ASN (s): -
CAIDA AS Rank: -
IXmaps AS rank: 29+

VIF internet is a carrier in Montreal, QC. VIF offers DSL internet connections for both residential and business. It also provides website hosting with emails and FTP services in addition to their VoIP service.

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**0**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**1**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://web.vif.com/terms-and-conditions/ (Undated)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Accepting	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	-

Virgin Mobile

Headquarters: Toronto, ON, Canada
Corporate parent: Bell[72]
Nationality: Canada
Corporate site:
http://www.virginmobile.ca

ASN (s): 30261
CAIDA AS Rank: 9059
IXmaps AS rank: 29+

Virgin Mobile is a subsidiary of Bell, using the Virgin brand. The company's Virgin Membership is designed to get customers special discounts at music festivals, retail stores, food, and movie theatres.[73]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**½**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.virginmobile.ca/en/support/legal-privacy.html?itcid=FOT:15 (Undated)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

[72] http://www.cbc.ca/news/business/bell-acquires-all-of-virgin-mobile-canada-1.810166
[73] http://www.virginmobile.ca/en/members-lounge/index.html

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	-	Yes	Yes

Wind Mobile

Headquarters: Toronto, ON, Canada
Corporate parent: Globalive[74]
Nationality: Egypt
Corporate site:
https://www.windmobile.ca/

ASN (s): 20365, 36273
CAIDA AS Rank: 7162
IXmaps AS rank: 29+

WIND mobile is a competitive mobile brand in Canada. The company is notable for offering no contracts and unlimited data on certain plans. Wind also offers cheap international calling and Unlimited US roaming. Wind's network operates primarily in Southern Ontario (including the Greater Toronto Area), Ottawa, Vancouver, Calgary, and Edmonton.[75]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**½**	
2) A public commitment to inform users of all third party data requests	-	**0**	
3) Transparency about frequency of third party requests and disclosures	-	**½**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**½**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**0**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: https://www.windmobile.ca/accessibility-and-terms/privacy-policy (Undated)
Transparency Report: http://www.windmobile.ca/docs/default-source/default-document-library/2013-transparency-report-wind-mobile.pdf (Undated)
Third Party Access Guidelines/Handbook: Not found

[74] http://www.theglobeandmail.com/report-on-business/wind-mobile-in-normal-situation-poised-to-acquire-spectrum-ceo/article22102740/
[75] https://www.windmobile.ca/why-wind/reasons-to-join

Notes:

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
Conditional	-	-

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

Xplornet

Headquarters: Woodstock, NB, Canada
Corporate parent: -
Nationality: Canada
Corporate site:
http://www.xplornet.com/

ASN (s): 22995
CAIDA AS Rank: 5842
IXmaps AS rank: 29+

Xplornet Communications Inc. (formerly Barrett Xplore Inc.) is a rural broadband provider in New Brunswick. Xplornet uses satellite and cell tower technology in order to provide 4G networks to rural areas without cable or DSL lines. The company has positioned themselves as Canada's "truly-national wireless broadband provider."[76]

Evaluation Criteria	Stars 2013	**Stars 2014**	
1) A public commitment to PIPEDA compliance	-	**0**	
2) A public commitment to inform users of all third party data requests	-	**½**	
3) Transparency about frequency of third party requests and disclosures	-	**0**	
4) Transparency about conditions for third party data disclosures.	-	**½**	
5) An explicitly inclusive definition of 'personal information'.	-	**0**	
6) The normal retention periods for personal information	-	**0**	
7) Transparency about where personal information is stored/processed	-	**0**	
8) Transparency about where personal information is routed.	-	**0**	
9) Domestic Canadian routing when possible	-	**1**	
10) Open advocacy for user privacy rights	-	**0**	

Primary Sources:
Primary Privacy page: http://www.xplornet.com/legal/xplornet-privacy-policy/ (Last revised: 2015)
Transparency Report: Not found
Third Party Access Guidelines/Handbook: Not found

Notes:

[76] http://www.xplornet.com/about-us/

Presence at Canadian Public IXPs

TorIX- Toronto	**OttIX - Ottawa**	**YYCIX - Calgary**
-	-	Invited

Appearance in other transparency reporting initiatives:

2013 IXmaps report	Citizen Lab study	AMI tool	CILP study
-	Yes	Yes	-

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@uoit.ca> is an Assistant Professor in the Faculty of Social Science and Humanities at the University of Ontario Institute of Technology. He also serves as a Research Associate at the Quello Center for Telecommunication Management and Law at Michigan State University. 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 (SSHRC), the Office of the Privacy Commissioner of Canada (OPC) and the Canadian Internet Registration Authority (CIRA), and is affiliated with the New Transparency Project and the Information Policy Research Program at the Faculty of Information, University of Toronto.