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

Report embargoed until:

March 12, 2015

IXmaps.ca
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.

‘Keeping internet users in the know or in the dark: A report on the data privacy transparency of Canadian internet carriers’ is licensed under a

Creative Commons Attribution 3.0 Unported License
http://creativecommons.org/licenses/by/2.5/ca/

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

---

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

KEEPING INTERNET USERS IN THE KNOW OR IN THE DARK?
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 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.

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. 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.

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

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.

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.

---

5 In the case of criterion 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.
7 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.
8 http://IXmaps/explore
Key Findings

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. Carriers are also being more publicly 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.

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,

---


Keeping Internet Users in the Know or in the Dark? 5
it appears that many Canadian internet carriers are in violation of their legal responsibilities under PIPEDA.

Policy 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 do more to generally promote 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 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, and

Recommendation 10: How they advocate for their subscribers’ privacy rights.

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.


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.