# GLOBAL INFORMATION SOCIETY WATCH 2014

*Communications surveillance in the digital age*

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

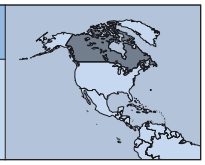
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

# CANADA

Surveillance and metadata collection in Canada



**Alternatives**
Catherine Pappas and Stephane Couture
www.alternatives.ca

## Introduction

Following revelations from US spy contractor Edward Snowden, it has become increasingly clear that Canada's intelligence agencies are routinely collecting personal data from a variety of sources for both political and economic reasons. In October 2013, a journalist associated with the British newspaper *The Guardian*, Glenn Greenwald, exposed how the Communications Security Establishment of Canada (CSEC) was monitoring Brazil's mining and energy industries, possibly on behalf of Canadian mining corporations. A few weeks later, new documents leaked to the Canadian Broadcasting Corporation (CBC) revealed that the Canadian government allowed the US National Security Agency (NSA) to conduct widespread surveillance while world leaders met at the 2010 G8 summit in Huntsville and G20 summit in Toronto. But allegations earlier this year about CSEC spying on airline passengers have hit closer to home, creating a great deal of concern over the nature of the government's surveillance activities.

Using the case of CSEC's collection of metadata through public airport Wi-Fi networks as a concrete example, this report will provide an analysis of the political and legal framework for understanding privacy and data protection laws and regulations in Canada in the age of ubiquitous surveillance. Looking at changes in technology, laws and regulations as well as political practices, it will try to show how some of today's trends have potentially serious implications for Canadian democracy.

## Policy and political background

Privacy in Canada is a fundamental but not an absolute human right. The right to privacy has always been measured with respect to other rights or societal goals, such as prevention of crime and the need to protect national security. But in the post 9/11 era, anti-terrorism legislation reduced judicial controls and eliminated or weakened oversight. Combined with fast technological transformations, this has undoubtedly undermined the application of Canadian privacy and data protection laws and regulations. Today, many fear that the country is at a turning point with regard to the protection of privacy.

In December 2001, the "omnibus" Anti-terrorism Act (Bill C-36) reasserted the CSEC's authority, redefined its mandate and concealed it in law as an autonomous entity directly accountable to the National Defence Minister. Its budget grew from 96.3 million Canadian dollars in 1999 to an estimated 829 million dollars in 2014.[1] Most importantly perhaps, Bill C-36 introduced a new provision that allowed CSEC to request ministerial authorisation for intercepting private communications for foreign intelligence purposes,[2] giving the agency greater legal cover to undertake its actions.

Over the last decade, there have also been many attempts to implement new laws that would grant additional powers and tools to collect data and conduct investigations using new digital technologies. Introduced as a way to modernise investigative techniques (Bill C-74, in 2005), to combat criminal electronic communications (B-52 in 2010), child pornography (Bill C-30 in 2012), or cyber bullying (Bill-C13, in 2014), these so-called *lawful access* provisions would force telecommunications operators and internet providers to disclose information about subscribers without the need for a warrant or a judicial order and, in some cases, without the permission to notify them about the data collection. Faced with overwhelming opposition from Canadians, so far, none of these bills have been adopted.

## CSEC and the expanding scope of surveillance through metadata collection

A key policy issue given prominence these days is the legality of the Canadian government's vast metadata collection programmes. On 30 January 2014, a document initially leaked by Snowden and obtained by CBC News[3] revealed that CSEC has

1 Office of the Parliamentary Budget Officer. (2014). *Main estimates 2014-15*. www.pbo-dpb.gc.ca/files/files/2014-15_Main_Estimates_Report_EN.pdf

2 Parliament of Canada. (2001). *Statutes of Canada 2001: Bill C-36*. www.parl.gc.ca/content/hoc/Bills/371/Government/C-36/c-36_4/c-36_4.pdf

3 Weston, G. (2014, January 31). CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents. *CBC News*. www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

been collecting metadata to monitor the activities of public airport wireless internet users. The leaked document describes the data collection project that occurred for over a two-week period in a major Canadian airport. With this data, CSEC was able to track travellers several days after they left the airport and connected their wireless devices to other Wi-Fi systems in Canadian cities or US airports. It could also track back the travellers' whereabouts the days before their arrival at the airport. IP profiling was then used to map travel patterns and geographic locations over a period of time.

The leaked document described the CSEC operation as a trial run of a powerful new software programme, developed jointly by CSEC with the help of the NSA, that could track "any target that makes occasional forays into other cities/regions." Although the authorities in charge of the Wi-Fi systems have denied providing any data to the government, one analyst suggests that it was "presumably obtained with the cooperation of Canada's major telecom companies."[4] The leaked document also mentions a "proof of concept" – possibly a previous pilot project – in which a modest-sized city was "swept" and a telecommunications system providing services to some 300,000 users was accessed. The CBC report on the leak also mentions intentions of sharing technologies and data collected with official spying partners.

This Snowden leak on CSEC's metadata collection programme came several months after the Canadian daily, the *Globe and Mail*, revealed that CSEC has been collecting Canadian metadata on "telephone and internet traffic records".[5] According to documents obtained by the newspaper, metadata collection programmes were authorised under two ministerial directives (in 2005 and 2011) on the collection and use of metadata. In light of these revelations, many suspect that the Wi-Fi data collection programme is not an isolated case and that information continues to be collected from other public Wi-Fi hubs across the country indiscriminately, over longer periods of time, and without our knowledge, to create metadata trails of individual users.[6]

CSEC has been legally mandated to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence," to "provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada," and to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."[7] The agency also shares information it collects or acquires with the other members of the Five Eyes Intelligence community, that is, the US, the United Kingdom (UK), Australia and New Zealand.[8]

CSEC's operations remain one of Canada's best kept secrets. Contrary to other law enforcement and intelligence agencies, such as the Canadian Security Intelligence Service (CSIS – similar to the CIA in the US) and the Royal Canadian Mounted Police (RCMP), CSEC is not designated as an agency under the Access to Information Act and the Privacy Act and, because of this, does not allow independent oversight by the Information Commissioner and the Privacy Commissioner.[9] Its only oversight is from the CSEC Commissioner, a watchdog role currently held by retired Québec judge Jean Pierre Plouffe, who reports to and is accountable to the Minister of Defence. According to Wesley Wark, an expert on national security, intelligence and terrorism, "the performance of the CSEC Commissioner's function has been hamstrung by an inability to communicate to the Canadian public and by the long-drawn-out battle to bring sufficient agreed clarity to CSEC's legal mandate with regard to the interception of private communications under Ministerial authorization."[10]

Often described as the digital envelope that carries the actual content over networks, metadata is not data *per se*, but refers to all the information used to identify, manage, describe or route data over a given network. Metadata can contain the date, time, duration and location of a communication, phone number or internet protocol address, as well as the ID of the sender and the recipient. Even if metadata

4 Geist, M. (2014, February 4). Against Oversight: Why Fixing the Oversight of Canadian Surveillance Won't Solve the Problem. *Michael Geist*. www.michaelgeist.ca/2014/02/csec-surveillance-problem

5 Freeze, C., & Stueck, W. (2013, October 22). Civil liberties groups launch lawsuit again. *The Globe and Mail*. www.theglobeandmail.com/news/national/canadian-eavesdropping-agency-facing-lawsuit-from-civil-liberties-group/article14984074

6 McGuire, P. (2014, February 4). The Harper government insists it's legal to collect metadata. *VICE Canada*. www.vice.com/en_ca/print/the-harper-government-insists-its-legal-to-collect-metadata

7 Communications Security Establishment Canada (CSEC). (2013). What we do and why we do it. www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-eng.html

8 en.wikipedia.org/wiki/Five_Eyes

9 Cavoukian, A. (2003). *National Security in a Post-9/11 World: The rise of surveillance... the demise of privacy?* Toronto: Information and Privacy Commissioner/Ontario. www.ipc.on.ca/images/Resources/up-nat_sec.pdf

10 Wark, W. (2012). *Electronic Communications Interception and Privacy: Can the imperatives of privacy and national security be reconciled?* Ottawa: Office of the Privacy Commissioner of Canada. cips.uottawa.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf

does not reveal the content of a conversation, the massive collection of metadata and its cross-linking can reveal much of the values, relationships and activities of an individual. Experts argue that metadata can provide the agency with a fairly accurate snapshot of an individual user, but the government continues to deny that metadata collection violates privacy rights, playing on the dichotomy between content and metadata to justify its programme and sideline privacy concerns. "Metadata is information associated with a telecommunication… and not a communication," stated a briefing note to the then Defence Minister Peter McKay in 2011, right before he approved the ministerial directive on 21 November 2011.[11]

According to CSEC governing legislation moreover, the programme is allegedly conducted under its foreign intelligence mandate and CSEC cannot target Canadians or persons in Canada. On 29 January 2014, following the airport Wi-Fi metadata collection, the chief of CSEC, John Forster, argued that the agency's activities are only directed "at foreign entities, and not at Canadians or anyone in Canada,"[12] although he later stressed that CSEC "is legally authorized to collect and analyze metadata."[13]

Civil society actors and advocates for the privacy rights of Canadians, on the other hand, worry that this and other operations led by CSEC lack public accountability or oversight and do not respect its mandate. Interviewed by the CBC, the province of Ontario's Privacy Commissioner Ann Cavoukian stated that "this resembles the activities of a totalitarian state, not a free and open society."[14]

But civil society criticism of CSEC operations is not new. In October 2013, the British Columbia Civil Liberties Association (BCCLA), a Canadian nonprofit advocacy group, filed a lawsuit aimed at CSEC for "illegal search and seizure", requesting that the agency stop certain surveillance activities.[15] The BCCLA argued that the agency's metadata collection programme authorised by the minister revealed private information about Canadians or persons in Canada, which infringes Article 8 of the Canadian Charter of Rights and Freedoms, guarding against unreasonable search and seizure.[16] OpenMedia, a Canadian advocacy group very active on internet and information and communications technology (ICT) policies, has also supported the BCCLA's claim and launched a campaign against spying on Canadians.[17]

## Conclusion

The metadata collection case raises many questions pertaining to privacy rights in Canada. First, it shows that CSEC activities are far more expansive than previously believed. CSEC seems to be collecting metadata widely with the help of major telecommunications companies. In Canada, public agencies and private businesses have traditionally been subject to different privacy laws. The tighter privacy laws governing the state were meant to protect Canadians from pervasive surveillance. But now that information openly flows from one side to the other without this being regulated by our privacy laws (as the government allegedly acquired some of the bulk data from telecommunications companies without a legal warrant), it raises deep concerns for accountability. In addition to this, the introduction of new lawful access legislation giving law enforcement officials warrantless access to private online information poses an even greater threat to democracy and civil liberties in Canada. A positive note in this story is a recent judgment by the Supreme Court that ruled the disclosure of private online information to government and police without a warrant was unconstitutional, making a step in the right direction for the protection of privacy rights in Canada.[18]

Secondly, the case described above highlights the inability of Canadian laws and regulations to deal with metadata. As Canadian technology policy analyst Michael Geist has suggested, the fact that the government insists on the legality of the programme might indicate that the problem lies in the law itself rather than its application, as much of the legal framework fails to acknowledge the broader privacy implications of metadata. There are also considerable discrepancies in the definition of "personal information" found in privacy laws governing the private and public sector, as

11 Freeze, C. (2013, June 15). How Canada's shadowy metadata-gathering program went awry. *The Globe and Mail*. www.theglobeandmail.com/news/national/how-canadas-shadowy-metadata-gathering-program-went-awry/article12580225/?page=all

12 Forster, J. (2014, January 29). Letter to the Editor re: Globe and Mail editorial, January 29, 2014. *Communications Security Establishment Canada (CSEC)*. www.cse-cst.gc.ca/home-accueil/media/media-2014-01-29-eng.html

13 CSE. (2014, January 30). CSE statement re: January 30 CBC story. *Communications Security Establishment Canada (CSEC)*. www.cse-cst.gc.ca/home-accueil/media/media-2014-01-30-eng.html

14 Weston, G. (2014). Op. cit.

15 British Columbia Civil Liberties Association. (2013). Civil claim to the Attorney General of Canada, 22 October. bccla.org/wp-content/uploads/2013/10/2013-10-22-Notice-of-Civil-Claim.pdf

16 Ibid.

17 https://openmedia.ca/csec

18 R. v. Spencer, 2014. scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

well as within federal and provincial privacy legislation.[19] Furthermore, over the years, technological transformations have weakened many of the barriers that were used to protect the privacy rights of Canadians and have rendered obsolete some privacy laws and regulations. Discussions surrounding the legality of the metadata collection programme have therefore been based on interpretation and differing views without having a clear legal framework to work from.

A third area of concern is with the very mandate for Canada's spy agency. It has become increasingly difficult to delineate the borders of a telecommunications network based on national boundaries. From this perspective, how can one guarantee that this widespread collection of metadata remains within the geographic boundaries of CSEC's mandate?

## Action steps

There have been several positive steps taken by different legislative bodies in Canada to reassert the privacy rights of Canadians. The Senate Standing Committee on National Security and Defence, for instance, is examining CSEC's programme and potential areas of reform. Civil society groups, on the other hand, are leading campaigns that press for greater protection of privacy rights and open debate on the limits of metadata collection and geography. In May 2014, a coalition of civil society groups and academics released the Ottawa Statement, which sets out recommendations aimed at putting a stop to government spying on innocent Canadians.[20] But still much remains to be done for protecting the privacy rights of Canadians, including:

- Engaging in a full, transparent and participatory public process in order to ensure that laws and regulations pertaining to privacy and the protection of data are in compliance with the Canadian Charter of Rights and Freedoms and acknowledge the United Nations' reaffirmation of privacy as a fundamental human right.
- Cultivating a better understanding and consideration of the privacy implications of metadata, in particular the way massive collection and cross-linking of this information can reveal much of the values, relationships and activities of an individual.
- Ensuring greater oversight of the operations of CSEC and other surveillance agencies in Canada.
- Putting an immediate halt to plans for introducing further lawful access provisions that would allow for authorities to access metadata through telecommunications agencies without any warrant.
- Strengthening the involvement of civil society in favour of privacy rights through public campaigning, advocacy and education.

19 Lyon, D. (2014). *Transparent Lives: Surveillance in Canada*. Edmonton: Athabasca University.

20 OpenMedia.ca. (2014, May 22). Canada's leading privacy experts unite behind Ottawa Statement, offer high-level proposals to rein in mass surveillance. *OpenMedia.ca*. https://openmedia.ca/news/canada%E2%80%99s-leading-privacy-experts-unite-behind-ottawa-statement-offer-high-level-proposals-rein-mass