Canada's Bad Dream

ANDREW CLEMENT

ABRINSKY

TORONTO—Edward Snowden's June 2013 leak has shone unprecedented light on the dark underside of Internet connectivity. So far, however, Canada has remained a victim largely hidden in the shadows.

Much of the debate over the National Security Agency (NSA) revelations has focused on U.S. domestic surveillance of individuals never under suspicion. But whatever modest legal protections Americans may enjoy, all those outside the United States are classified as foreigners and have no such protection. And while we know most about the NSA's domes-

tic surveillance operations, the Snowden documents make very clear that with the aid of its allies—Great Britain, Canada, Australia, and New Zealand—the NSA has developed a globe-spanning surveillance infrastructure of remarkable scale and scope. Not surprisingly, the NSA has targeted countries regarded as "unfriendly" to American interests, such as China, Russia, and Iran, but the Agency has also been intercepting and analyzing the internal communications of countries generally regarded as "friendly" allies, such as Brazil, Denmark, Germany, France, India, Italy, Netherlands, Norway, Spain, and many more. The aptly named Boundless Informant program reported that in one month alone, the NSA's Global Access Unit collected data on over 97 billion emails and 124 billion phone calls from nearly every country.

HOW CANADA RESPONDS TO THE NSA-SNOWDEN CRISIS WILL DEFINE ITS IDENTITY AND SHAPE ITS FUTURE.

Rarely mentioned in the Snowden documents is the targeting of Canadians. But for a variety of geographic and historical reasons, Canada is at the forefront of NSA mass surveillance and a potential bellwether in terms of responding technically and politically to the challenge of unfettered state surveillance. Given its long shared border and the pattern of Internet buildout in North America, much of Canada's internal Internet traffic—domestic traffic that originates and terminates in Canada—is routed via the United States, where it is subject to the NSA's domestic interception programs. Furthermore, the lack of international submarine fiber optic cables on Canada's shores means that almost all of Canada's third country Internet traffic is similarly routed through the United States and via NSA surveillance operations.

Canada's reliance on the United States' Internet infrastructure for its vital communications presents an obvious threat to Canada's ability to protect the privacy of its citizens, as well as its sovereignty more broadly. This dependence also represents a significant departure from Canada's longstanding policies of maintaining its economic, social, and cultural independence in the face of U.S. expansionism that dates back to the founding of the nation in the mid-19th century. Indeed, Canada's nation building has been defined from its birth in terms of building its own unique national transportation and communications infrastructures. The first major initiative, popularly referred to as the National Dream, was the construction of a transcontinental railway to tie Canada's far flung western provinces to the heartland and pre-empt northward migration of American settlers and commercial links. Similar motives underpinned subsequent development of Canadian government policies and investments in broadcasting, telecommunication, air transportation, and other infrastructure. Even as recently as this millennium, the Canadian government invoked its historic

Andrew Clement is a professor in the Faculty of Information at the University of Toronto, where he coordinates the Information Policy Research Program and leads the IXmaps.ca research project.

legacy and mythology in its plans for Internet development in its report *The New National Dream: Networking the Nation for Broadband Access.*

DREAM TO NIGHTMARE

Now that we know that mass state surveillance capacities are being deeply embedded into our Internet infrastructure, Canada's dream of a universal and unifying communication network risks turning into a nightmare. How Canada responds to the NSA-Snowden crisis will define its identity and shape its future for decades to come.

Contemporary Canadian concerns over and reaction against the prospect of unfettered access to its data by the NSA and other U.S. government agencies date to the passage of the Patriot Act in 2001, in the immediate aftermath of the September 11 attacks. Particularly controversial—when the provisions became known in Canada—were the expansion of state surveillance powers, reduced judicial oversight, stiffened gag orders, and electronic data capture extending beyond U.S. borders. In the ensuing debate, two Canadian provinces changed their laws to bar public bodies from storing Canadians' data in the United States. The federal government also adopted a policy that all personal data it holds on Canadians must be stored within its own computers. On the other hand, the view that has prevailed more broadly is that because of the mutual legal assistance and other information sharing agreements between the two countries, storage at home in Canada provides no greater protection for Canadians' data. While hardly reassuring about the privacy protections many Canadians took for granted, this liberal approach to data flowing south across the border has facilitated the growth of U.S.-based cloud services and outsourcing.

However, recent revelations of the astonishing scale of the NSA's hitherto secret surveillance activities and the remarkably broad legal interpretations it uses to justify them, are now leading to a re-consideration of this view, with potentially wide consequences.

Under the PRISM program, which involves tapping directly into the servers of nine leading U.S. Internet companies, the fine grained and potentially sensitive data these social network and cloud services collect and store is subject to NSA access, regardless of location. Starting in 2007, the NSA had arranged PRISM partnerships with the largest Internet companies, notably Microsoft, Yahoo, Google, Facebook, and Apple. Canadians' widespread use of their popular services in effect turns over vast repositories of personal data for unfettered NSA mining.

SPY & SWITCH?

The obvious way of avoiding this form of privacy risk is to switch to similar services based outside the United States. Canadian Internet companies were quick to see a competitive advantage in being beyond the NSA's apparent reach, and soon after the first Snowden publications began advertising their services as more secure and privacy protected. Canada's largest telecommunications enterprise, Bell Canada, began touting itself in July 2013 as keeping "your data safe, secure, and stored in Canada":

"When it comes to data security, location matters. The laws governing data centres outside of Canada can be different—and less protective—than those here at home.

"Bell data centres are 100 percent Canadian owned and operated. We keep your data secure, under the protection of Canadian

government regulations, and hosted in facilities that meet top industry certifications."

As foreign governments, corporations, and individuals become more aware of the risks of NSA surveillance, the nine companies most prominently implicated in the American government spying are seeing their financial prospects under threat, with projected business losses estimated in the billions. They are beginning to fight back, by challenging the U.S. government to curtail its reach while actively promoting their own services in Canada.

Google and Microsoft, in particular, are continuing to woo Canadian universities with offers of free email and other e-communications services, an attraction for cash-strapped public institutions. While before the Snowden leak, faculty members who opposed the outsourcing of institutional e-mail failed in their attempts to halt these initiatives, the terms of the debate are now changing significantly. The concept that constitutional protections found in Canada's Charter of Rights and Freedoms take precedence is beginning to play an increasing role in forming national opinion toward the revelations of the extent of American collection of data originating north of the border. The recent unanimous Supreme Court of Canada decision in the Spencer child pornography case, which found that Canadians have rights to anonymity when online and that law enforcement needs warrants to access personal internet subscriber data, has further strengthened the case for keeping data away from the United States.

BOOMERANG ROUTING

While the controversy in Canada has mainly focused on the storage of data in the United States or by firms covered by U.S. jurisdiction, interception of data while in transit is more recently becoming an issue. Internet traffic does not always follow the shortest geographic route, mainly due to the interconnection arrangements of the major international carriers. However, the extent of this practice and its surveillance implications are less well known. While this affects many countries, Canadian traffic, largely due to its proximity to the United States, as well as the structure of the North American Internet service industry, is especially prone to routing via the United States.

We refer to traffic that originates and terminates in the same country, but transits through another, as "boomerang traffic." Since 2009, the IXmaps.ca research project, based at the University of Toronto, has been collecting and mapping the routes data packets take across the Internet ("traceroutes") and through sites of suspected NSA Internet surveillance.

With the cooperation of corporate personnel, the NSA splices optical 'splitters' into the high capacity fiber optic cables at major internet switching centers. These are half-silvered mirrors that allow the signals to proceed, while directing an exact copy of all the traffic passing through these links into machines that can analyze and forward to the NSA for storage. In other words, this operation enables the NSA to monitor not only who is communicating with whom, but potentially the entire content of these communications as well. One known location of such a splitter operation is AT&T's main switching center in San Francisco. At least 17 other U.S. cities are also very likely to host similar NSA interception facilities.

Analysis of the 30,000 traceroutes now stored in the IXmaps database strongly suggests that at least a quarter of the Canadian routes follow a boomerang pattern. That long distance Canadian communica-

tions may be routed via the United States is not surprising, but the number of routes that start and end in the same Canadian city and are also routed via the United States is striking. More than 100 such boomerang routes are based in Toronto alone.

Whether crossing the continent, or simply crossing the street, Canadian boomerang traffic is almost entirely exposed to NSA surveillance. Given their size and proximity to the Canadian border, the main American cities for boomerang routings and NSA interception are New York, Chicago, and Seattle, but boomerang routes can be found in many other U.S. cities, including San Francisco, Los Angeles, and even as far south as Miami, all among the cities most suspected of hosting NSA splitter operations.

In tracing patterns of boomerang routing, it might be expected that geography largely dictates the outcome. Since Internet backbone capacity is much greater south of the border, it makes some sense to find that routes between the West and East coasts of Canada or between Vancouver and Toronto go via the United States. However, geography clearly does not account for boomerang routes whose endpoints are across the street from each other, and pass through the same Internet switching center going to and from the United States.

One explanation may be found in the particular carriers involved. In brief, carriers are selective about their direct traffic exchange partners. The larger carriers typically are reluctant to exchange traffic with their smaller competitors and have an incentive to make it difficult for them to reach destinations outside their immediate networks. One effect of these business practices is to force a considerable amount of Canadian Internet traffic onto the networks of large American carriers, such as Cogent, Hurricane, and Level 3, as well as Tata (Indian) and TeliaSonera (Swedish). These foreign carriers typically meet the large Canadian carriers for data handoffs at major Internet switching centers in large U.S. cities, just the locations where the NSA has a strong incentive to install its interception facilities.

The close correlation between boomerang routing and contractual arrangements between Internet service providers (ISPs) around inter-carrier routing means that all Canadian Internet users are touched in some fashion—a factor in nearly every type of web-based transaction across the full range of service organizations that Canadians use in their everyday affairs. IXmaps suggest citizens interacting online with their federal and provincial governments, as well as doing online banking and many other everyday Internet transactions, will often be exposed to boomerang routing with its potential for NSA surveillance. Making such material available to the NSA or any other state security agency understandably can produce a most uncomfortable feeling, to say nothing of eroding basic privacy rights.

THE WIDESPEAD BOOMERANG ROUTING RAISES SERIOUS CONCERNS NOT ONLY FOR THOSE CONCERNED WITH CANADIANS' PRIVACY, BUT ALSO FOR THOSE SEEKING TO ADVANCE THE VITALITY OF CANADA'S TECH INDUSTRY AND INFRASTRUCTURE MORE BROADLY.

This loss of control of personal information and evident lack of accountability on the part of the organizations handling

ACTION STEPS

- Develop and promote the use of Canadian public Internet exchange points (IXPs).
- Open access to Canada's long-haul Internet backbone, especially to facilitate traffic between public IXPs.
- Require Internet service providers in contracts with public bodies to include open peering at public IXPs where available.
- Re-examine, in light of the Snowden revelations, the issue of privacy protection for Canadians' personal data when exposed to U.S. jurisdiction.
- Require greater transparency and accountability by Canadian telecom carriers in terms of their inter-network routing practices, long haul carriage capacity and utilization, and data-protection provisions in the contractual arrangements with transit providers.
- Require greater accountability and transparency on the part of the security and intelligence community in Canada via parliamentary discussions.

—Andrew Clement

it represents a significant privacy invasion and violation of the personal data protections found in Canadian law—notably the Personal Information Protection and Electronic Documents Act (PIPEDA), as well as the Canadian Telecommunications Act, which has among its primary objectives "to contribute to the protection of the privacy of persons."

DOT-CA

The widespread boomerang routing raises serious policy issues not only for those concerned with Canadians' privacy, but also for those seeking to advance the vitality of Canada's tech industry and infrastructure more broadly. The Canadian Internet Registration Authority (CIRA) has as its mission to "foster the development of .CA as a key public resource for all Canadians by providing stable, secure, and trusted domain name services, and by taking a leadership role in shaping Canada's Internet for the benefit of .CA domain holders." Yet dependence on American routing of Canadian Internet traffic is inefficient and impairs the ability of Canadian Internet users to enjoy high quality Internet services. Well before the Snowden revelations, CIRA commissioned an expert study of the Canadian Internet infrastructure, which compared all-Canadian routings with those that transited the United States and found significant inefficiencies with the boomerang routing.

CIRA's report concluded that "Canadian Internet access is heavily and unnecessarily dependent upon foreign infrastructure, especially U.S. infrastructure." It then went on to conclude that boomerang routing "imposes significant burdens on Canadian Internet users," in the form of higher service prices, slower network speed, and greater likelihood that "the data is subject to examinations by companies and government authorities in those countries."

It's not only Canada-to-Canada Internet traffic that is subject to an American

boomerang. Most Canadian Internet communications with countries other than the United States have similar boomerang characteristics, in the sense that the traffic passes through the United States, usually via a city where the NSA has splitter interception facilities. The reality is that only two trans-Atlantic fiber optic cables land on Canada's East Coast, compared with 12 landing in the United States. There are no trans-Pacific fiber optic cables landing on Canada's West Coast, while 13 land in the United States.

CANADA FOR CANADIANS

Citizens' ability to communicate freely and openly with their own government and fellow citiziens is central to the concept of a democratic society. Conversely, the inability for an individual to avoid compromised communication channels, such as represented by boomerang routing and accompanying risks from NSA surveillance, calls into question the government's capacity to protect the integrity of its communications, erodes trust in vital governmental institutions, and ultimately undermines the legitimacy and sovereignty of the state. This is well recognized in Canada's Telecommunications Act, which affirms that Canadian telecommunications services play "an essential role in the maintenance of Canada's identity and sovereignty."

There are several ways to address the threat of foreign mass Internet surveillance and NSA interception in particular. This would involve a combination of infrastructure, administrative, and legal changes. Keeping Canadian domestic Internet communication within Canadian jurisdiction and subject to its constitutional and data protection regimes will require the development of greater technical capacity to route traffic efficiently through domestic facilities. These include, most notably, establishing public Internet exchange points, where all carriers can freely hand traffic off to each other, as well as acquiring access to high capacity fiber optic trunk lines that connect them. The new exchange points would enable the various local networks, such as retail ISPs and institutional networks, to reach end users on other networks, without having to depend on buying transit services from foreign carriers.

CIRA has taken the lead in this approach, by acting as a catalyst for the development of more Internet exchange points (IXPs) across Canada—identifying the key benefits of cutting operating costs, raising bandwidth available to Canadian users, reducing the risk of Canadian data becoming subject to foreign jurisdictions, and improving reliability and resilience to natural disasters and attacks. Though CIRA observes that while "IXPs typically cost less than $100,000 to establish, and return on investment can be seen in as little as a few days," Canada is far behind other countries in developing IXPs. In 2012, the United States had 85, while Canada had just two. CIRA plans to open three more by March 2015, and identifies five more as high priority.

DEVELOPING ADDITIONAL CANADIAN INTERNET EXCHANGE POINTS AND OPENING ACCESS TO LONG HAUL TRANSMISSION CAPACITY WILL MAKE IT CHEAPER AND EASIER FOR ISPS TO KEEP CANADIAN DATA AT HOME.

Opening access to trans-Canadian Internet backbone capacity would help

avoid boomerang routing. The topic of Internet capacity and congestion is hampered by a lack of accurate public reporting on infrastructure capabilities and performance, in part because this information is treated as proprietary and competitive. In contrast to the need for financial investment and physical construction in the case of developing more Internet exchange points, expanding effective long haul backbone capacity for avoiding U.S. routing is more a matter of obtaining access rights to existing fiber lines than it is in laying more of it. Should public funds be required, these appear to be available if there were a change in priorities. In sharp contrast to the nearly $1 billion the federal government has appropriately invested in extending Internet services to rural and remote areas over the past decade, no comparable financial commitments have been made to ensuring that Canada has a high capacity, widely accessible Internet backbone that serves the greater public interest effectively.

While developing additional Canadian Internet exchange points and opening access to long haul transmission capacity will make it cheaper and easier for ISPs to keep Canadian data at home, these measures alone won't guarantee that result. The purchasing power of public institutions offers another legitimate and potentially powerful means to encourage domestic routing. The federal government's policy on contracting states the intention to "support long-term industrial and regional development and other appropriate national objectives." A general procurement requirement that contractors providing Internet routing services examine carefully Canadian Internet points would repatriate a significant portion of traffic that currently travels via the United States. If Canadian governments all peered openly at IXPs, it would provide a potent example and incentive for others to follow suit. It would also likely save money for the public purse, as well as for those interacting with government over the Internet.

PROTECTING PRIVACY

Existing Canadian laws, notably PIPEDA, as well as similar provincial and public sector laws, require that when a data custodian passes personal information to a third party, the custodian must ensure that the data enjoys comparable or higher levels of protection. The weaker legal protection Canadian data enjoys in the United States and the overwhelming evidence that the NSA has access to foreigners' data passing through the United States strongly suggest that Canadian carriers routing domestic Internet traffic south of the border or simply handing data over to U.S. companies inside Canada for domestic delivery are not complying with Canadian law.

More proactive disclosure by Internet service providers of the terms of data agreements between contracting parties is essential. Another important privacy measure is to increase the use of encryption for data transmission and storage, making it much more difficult for any third party to access the content of a communication. In response to the Snowden revelations, the tech community is actively developing and promoting more reliable and easier to use encryption tools. Major Internet companies, such as Google, are also making currently available encryption capabilities the default for communication rather than the exception. Growing adoption of encryption would significantly raise the cost of surveillance and force security agencies to shift away from their current population-wide dragnet approach to

concentrate their efforts on targets where there was substantial suspicion. All such measures will likely prove feasible and effective, even necessary, in significantly reducing the flows of Canada's domestic Internet traffic that transits the United States and is hence exposed to NSA surveillance. Of course, these policy measures, even if adopted in full, are far from sufficient in addressing the many other challenges of mass state surveillance. They do not tackle the NSA's surveillance programs that through partnerships with major online service providers popular with Canadians, enable relatively direct access to troves of stored personal data. Furthermore, by concentrating more domestic traffic within Canada, they make more urgent the necessity of an informed national dialogue aimed at resolving the thorny issues around Canada's own suspicion-less mass surveillance program, and in particular the role of its NSA counterpart, the Communication Security Establishment Canada (CSEC).

To secure Canadian domestic Internet communications from unaccountable state security agency intrusion, we need progress on both fronts, so in this sense efforts would complement each other.

Finally, whatever success is achieved in better protecting domestic communications, there will remain a vital public interest in ensuring safe, free, open global Internet communication. This will require developing a robust international regime for protecting online privacy and free expression—the hallmarks of democratic societies. Canadians can still pursue their national dream while forging in our highly connected world a progressive compromise among the contending actors—building a stronger nation as a leading member ofthe world community. ●

Thanks to colleagues in the IXmaps research team, most immediately Jonathan Obar, Colin McCann, Antonio Gamba-Bari, to friends who provided valuable comments on draft versions, and to funders SSHRC, OPC, CIRA.