CHAPTER I

Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges[1]

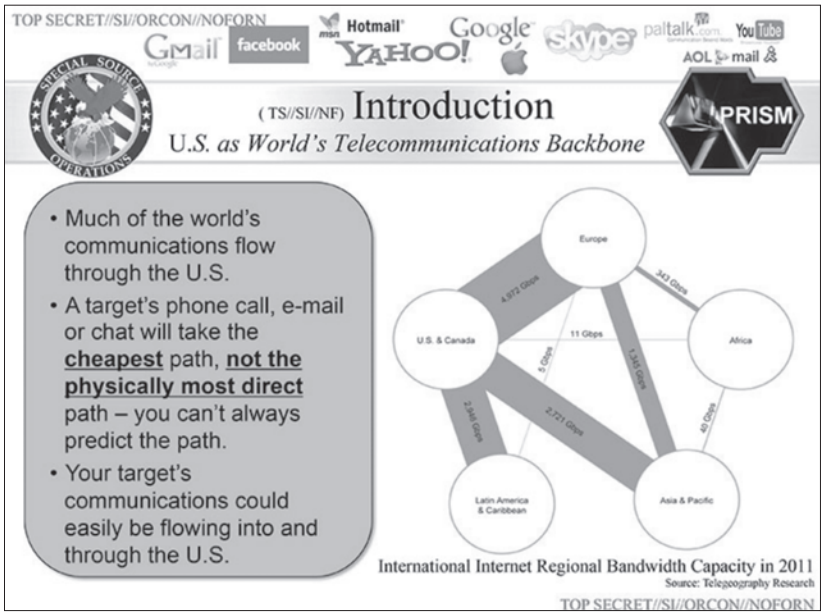
Andrew Clement and Jonathan A. Obar

Introduction

The 2013 revelations of US National Security Agency (NSA) surveillance programs that whistle-blower Edward Snowden's release of hitherto secret internal documents brought to public attention have sparked a storm of controversy.[2] Their breathtaking scope, scale, and questionable legality have led many countries to urgently assess the risks of NSA surveillance and to consider various actions to better protect the privacy of their citizens as well as their national sovereignty.

Given the large proportion of international Internet communications routed through the United States[3] where foreigners' data receives scant legal protection, a major focus of controversy is the NSA's mass (near total) Internet traffic interception capability.[4] Besides the extraordinary technical prowess the United States is able to deploy in the service of its perceived surveillance and security needs, it also enjoys a strategic advantage in that a disproportionate share of international data communications passes through it. This is an advantage the NSA is well aware of, as noted in a presentation deck for the top-secret PRISM program: "Much the world's communications flow through the U.S. …Your target's communications could easily be flowing into and through the U.S." See Figure 1.[5]

Figure 1: U.S. as World's Telecommunications Backbone



Source: Washington Post

Well-founded suspicions about this surveillance potential have been reported for years, but the Snowden revelations now strongly reinforce the serious allegations of clandestine spying that author James Bamford, retired AT&T technician Mark Klein and others have raised.[6] Given Canada's proximity to the United States and the structure of the North American Internet, it isn't just Canada's international traffic that is subject to suspicionless, dragnet NSA surveillance. Due to a phenomenon we term "boomerang routing"[7] — when Internet traffic originating and terminating in the same country transits another — a great deal of Canadian domestic Internet communications boomerang through the United States and are subject to NSA surveillance.[8]

This chapter examines the phenomenon of Canada-to-US-to-Canada boomerang traffic, focusing specifically on the privacy and related risks associated with NSA surveillance as well as the policy implications and remedial responses. As public understanding of how the Internet operates is generally inadequate for discussing the policy dimensions of Internet backbone surveillance, we begin with a brief overview of the technical aspects of Internet routing and then

show how surveillance capabilities can be built into relatively few "choke points" yet capture the great bulk of Internet traffic. In contradistinction to the common metaphor of the Internet as a spaceless, featureless "cloud," we demonstrate that, with interception points in under twenty major cities, the NSA is capable of intercepting a large proportion of US Internet traffic. We turn then to Canadian Internet routing patterns, showing that boomerang routing is commonplace, that such routing exposes Canadians' data to NSA surveillance, and that Internet users across Canada conducting a wide range of everyday communications are subject to it. Even communications between public institutions across the street from each other can be routinely exposed to NSA interception. Both to collect data about these Internet routing patterns and reveal its physical, geographic characteristics, we draw on a research-based Internet analysis and visualization tool known as IXmaps, developed to map Internet exchange points and the traffic routed through them. The software tool found at IXmaps.ca[9] aggregates crowd-sourced Internet users' "traceroutes" and shows them where their personal traffic is likely to have been intercepted by the NSA.

The next section considers the policy implications of Canadian boomerang traffic, especially from the point of view of its privacy risks. We also consider the economic inefficiencies and point to the broader issue of the impairment of Canada's network sovereignty. The final major section offers possible remedies for the various negative aspects of boomerang routing. To reduce boomerang traffic, we propose several ways for keeping domestic data within Canadian networks and legal jurisdiction. Building public Internet exchange points in Canada would contribute to keeping domestic traffic inside national boundaries while promoting more efficient routing. To mitigate the privacy and democratic governance risks in particular, we advance ideas for greater transparency and accountability on the part of telecommunications carriers and government agencies. While recognizing the need to address the risks from mass surveillance by Canadian state agencies as well as to develop stronger international regimes for protecting privacy, freedom of expression, and civil liberties online, we close by calling for a greater assertion of Canadian network sovereignty within the norms of a free and democratic society.

NSA Interception of Canadian Internet Traffic

The almost weekly revelations from the Snowden trove of yet more NSA surveillance programs contributes to the strong and accurate impression that the NSA has largely succeeded in Director Keith Alexander's reported mission to "collect it all,"[10] and developed a global, ubiquitous spying infrastructure capable of capturing the details of nearly everyone's electronic transactions. However, it is hard for all but the most dedicated and technically sophisticated observer to keep track of the various programs and their particular characteristics. The details matter in terms of who is targeted, the types of information collected, the relevant legal jurisdictions, the parties implicated and the possible remedies. The PRISM program in which the NSA has partnered with nine major Internet companies, such as Google, Facebook, Twitter, Microsoft, and Apple, to obtain "direct" access to stored personal data, is among the best known.[11] However, the NSA programs that intercept Internet communications in transit, while less well reported, are arguably the most significant in terms of their potential impact because they can capture data from all Internet users across a wide range of on-line activities. It is these programs for capturing data "on the fly" that we examine in this chapter. To understand them and their implications, it is helpful to understand how Internet data is routed.

The Internet Is Not a Cloud: Routing Basics

Unlike the telephone system, which relies on establishing a continuous dedicated circuit between the two ends of the communication path, all Internet communication is based on packet switching. Every e-mail message, voice conversation, video, image, web page, etc., is broken into in a series of small data packets. Each packet consists of two parts: a header, containing among other items, source and destination IP addresses, much like the return and to addresses on a conventional piece of mail; and a payload, containing the content. Each packet "hops" from the originator through a succession of routers, with each router examining the packet header to determine the destination and then passing the packet to the next router in the intended direction, again much like the conventional postal service routes mail. At the destination, the packets are reassembled into the original message. The response, whether it is a web page, video, file transfer, etc., consists of another set of data packets, that

individually hop their way through a succession of routers back to the originator. These routers and the links between them constitute the Internet backbone.

It is commonplace to refer to the Internet as a "cloud," as a seemingly boundaryless ethereal space in which physical location of wires and equipment is largely irrelevant. While this metaphor may be helpful in marketing Internet services, it does not well serve understanding how the Internet actually works, especially in matters of public policy around state surveillance. In fact, Internet traffic switching is mainly done by massive banks of routers crammed into large anonymous buildings located in the downtown core of major cities. These switching centres are linked by bundles of fibre optic cables each capable of transmitting tens of billions of bits per second[12] Mainly large telecommunication companies own these cables and routers, and the policies they adopt for who can connect to their networks and on what terms fundamentally determines how the Internet operates. And gaining access to the routers and cables to intercept the data packets streaming through them for surveillance purposes typically requires obtaining the cooperation of these often giant telecommunications enterprises.

NSA Internet Backbone Surveillance

The New York Times first reported the interception of US domestic communications by the NSA in late 2005.[13] But it wasn't until Mark Klein, a recently retired AT&T technician, revealed the existence of a secret "splitter" operation at 611 Folsom St. in San Francisco that the scope and technical details of NSA surveillance came to public light. Klein reported that AT&T had spliced fiber optic splitters into sixteen "peering links" that connected its network with other major carriers and Internet exchange points, directing an exact copy of all the traffic passing through these links into a "secret room" on the sixth floor, Room 641A. Here a deep packet inspection device, the Narus STA 6400, analyzed all the packets passing by, providing "complete visibility for all Internet applications," according to its vendor.[14] In other words, this operation enables the NSA to monitor not only who is communicating with whom, but potentially the entire contents of these communications as well.

Klein's revelations provoked strong reaction by civil liberties organizations, resulting in over forty court cases against US telecom carriers and the federal government. These cases allege that the

carriers illegally complied with multiple surveillance requests from the NSA during the Bush administration to provide without warrants specific information about US citizens.[15]

The secrecy that pervades this topic makes it difficult to determine whether the NSA surveillance program is continuing or not, but the recent reports strongly suggest that not only is it ongoing, but is expanding during the Obama administration. James Bamford's article in the March 2012 issue of *Wired* details the construction of an enormous data centre in Bluffdale, Utah, capable of storing and analyzing the complete record of interpersonal Internet traffic.[16] In July 2012, three whistle-blowers, William E. Binney, Thomas A. Drake, and J. Kirk Wiebe, all former NSA employees, gave evidence in the Electronic Frontier Foundation's (EFF's) (2012) lawsuit against the government's mass surveillance program, *Jewel v. NSA* in support of the surveillance allegations. In particular, Binney, a former NSA technical director, claims the then current program, known as Stellar Wind, was capable of intercepting virtually all e-mail in the United States and much else.[17] The more recent revelations by whistle-blower Edward Snowden further confirm the earlier claims and identify this form of interception as part of the "Upstream" suite of surveillance programs.

Given that the NSA's Internet surveillance is ongoing but its details still a closely guarded secret, how can we determine where it is being conducted, and whose traffic is capable of being intercepted? These are the central questions we now examine. We will focus our investigation on AT&T, and the splitter installation at 611 Folsom Street, as this is the best documented case and provides a model for the interception of Internet traffic at other major Internet exchange points in the United States and presumably by other major carriers.

Where Are the NSA Splitter Sites?

While we know of the NSA splitter site at 611 Folsom Street, what about additional suspected sites? Based on his conversations and meetings with other AT&T technical staff, Klein reported that similar installations were installed in five other locations — Seattle, San Jose, Los Angeles, San Diego, and Atlanta.[18] However, these six sites would not be sufficient to comprehensively intercept US Internet traffic, as there are other, more important routing centres that would be much more attractive for interception purposes. Scott Marcus, a former Federal Communications Commission expert, estimated that

AT&T had fifteen to twenty splitter sites.[19] However, he wasn't able to identify any sites in particular without further specific evidence. Presuming that the NSA's goal was to be able to intercept the largest proportion of US Internet traffic with the fewest possible sites (a hypothesis well confirmed by the subsequent Snowden revelations), we developed a rough schema for scoring cities based on how much Internet traffic was likely to pass through them. Using only our personal estimates of three determinants of Internet prominence, with crude relative weightings — telecom infrastructure (10); city size (population) (5); and geographic location in relation to other major population centres and telecommunications traffic patterns (4) — we developed an ordered ranking of the US cities most likely to host an NSA splitter installation.[20]

To test our hypothesis, and more generally provide a means for Internet users to see where their data travelled and was possibly subject to surveillance, we developed the IXmaps software system. Using a crowd-sourced approach, we invite geographically scattered users to install a customized version of the common traceroute program that populates our database.[21] We add location data for the routers encountered using a variety of standard geolocation techniques and from this users can then selectively map their own or others' traceroutes via a Google Maps mash-up. In early 2015, the database contained over 36,000 traceroutes contributed by more than 300 submitters from over 340 originating addresses (mainly in North America) to in excess of 2,800 destination URLs. We examined all the US-only routes in the IXmaps database, which numbered 4,200. Of these, 4,068 passed through at least one of the 18 cities we identified as the most likely sites for NSA splitter operations. In other words, installing splitters in the major Internet exchange points in just these cities would be sufficient for the NSA to intercept 97 percent of our US only traceroutes! These are shown in Figure 2.

While this result does not prove that these cities actually have NSA splitter operations, nor that the NSA has access to all the Internet exchange points in them, it is powerful confirmation that if the NSA installs splitters in relatively few strategic Internet choke points, it would be technically feasible for it to intercept a very large proportion of US Internet traffic. This high percentage helps justify our claim that these cities are strongly suspected of hosting NSA warrantless surveillance facilities. It also vividly challenges the popular image of the Internet as a "cloud."

Figure 2: 18 US Cities most likely to Host NSA Splitters[22]

Source: IXmaps

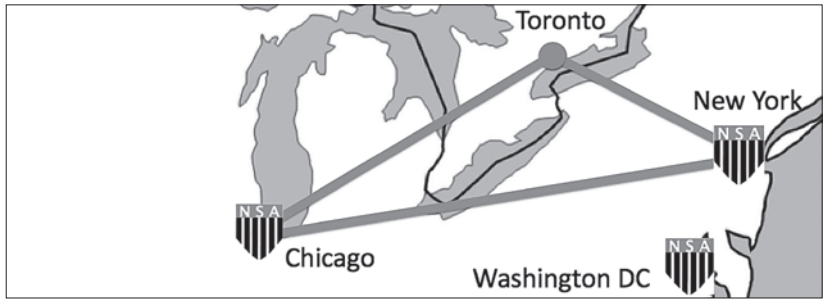
Canadian Boomerang Routing

So far we have concentrated on showing how and where the NSA can intercept Internet traffic within US borders, but how does this relate to Canadian domestic traffic? One of our discoveries in the IXmaps project is that a relatively large number of the traceroutes in our database that originate in Canada and terminate in Canada pass through the United States along the way. We refer to these as boomerang routes because the transmissions often travel considerable distances away from the sender before arriving at a receiver who is not nearly as far from the sender as the transmission path would suggest. While this phenomenon is familiar to those in the Canadian Internet routing business, its scale, causes, and implications are not well known more widely.

For example, a particularly revealing example of boomerang routing is depicted in Figure 3, showing a route that begins and ends in Toronto, between the University of Toronto and the Ontario government nearby, but passes through New York and Chicago. (The shield icons indicate cities with suspected NSA splitter operations.)

In early 2015, the IXmaps database contained 9,233 traceroutes that originated and terminated in Canada, and, of those, 2,049, or 22 percent, boomeranged through the United States. Nearly all of these boomerang routes passed through at least one of the cities

Figure 3: A Canadian Boomerang Route Based in Toronto: UofT <> OSAP



Source: IXmaps.ca/explore TR6896

we identified as containing NSA splitter operations. This pattern of high likelihood of NSA interception of Canadian boomerang traffic has been consistent over the several years we have tracked this phenomenon.[23] Given their size and proximity to the Canadian border, unsurprisingly the main US cities for boomerang routings are New York, Chicago, and Seattle, but we also found boomerang routes through many other US cities, including San Francisco, Los Angeles, and even as far south as Miami.

In attempting to account for patterns of boomerang routing, one might expect that it is largely a matter of geography. Given that Internet backbone capacity is much greater south of the border, it makes some sense to find routes between the West and East Coasts or between Vancouver and Toronto that boomerang.

However, geography clearly does not account for the frequent occurrence of routes that start and end in the same city but nevertheless transit the United States, such as the example above. In that case, the endpoints are across the street (Queen's Park Circle) from each other, and pass through switching facilities at 151 Front Street both to and from the United States. To help explain this curious phenomenon we need to take account of the particular carriers involved. In brief, carriers are selective about who they exchange traffic with directly: the larger ones 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. As Internet expert William Norton describes in *The Internet Peering Playbook*, dominant Internet carriers adopt this oligopolistic strategy.[24] One of the most visible illustrations of this is the fact that

while many smaller Canadian ISPs offer the chance to peer openly at public Internet exchange points, such as the Toronto Internet Exchange (TorIX) housed in 151 Front Street, none of the major ISPs (e.g., Bell, Rogers, Telus) do so.[25]

One effect of these business practices is to force a considerable amount of Canadian Internet traffic onto the networks of large US carriers such as Cogent, Hurricane Electric, Level 3, as well as Tata (Indian) and TeliaSonera (Swedish). These foreign carriers typically, but not exclusively, meet the large Canadian carriers for data handoffs in the United States.[26]

IXmaps Boomerang Findings

The close correlation between boomerang routing and contractual arrangements between ISPs around intercarrier routing means that it touches all Canadian Internet users, regardless of where they are located and which ISP they directly subscribe to. For the same reason, it is also a factor in nearly every type of web-based transaction across the full range of service organizations that Canadians rely on in their everyday affairs. To illustrate this we draw on IXmaps examples of citizens interacting online with their federal and provincial governments as well as online banking and other everyday Internet transactions.

A citizen's ability to communicate freely with government and fellow citizens is central to the concept of democracy. This is one reason that Canada's *Telecommunications Act* of 1993 affirms that Canadian telecommunications services play "an essential role in the maintenance of Canada's identity and sovereignty."[27]

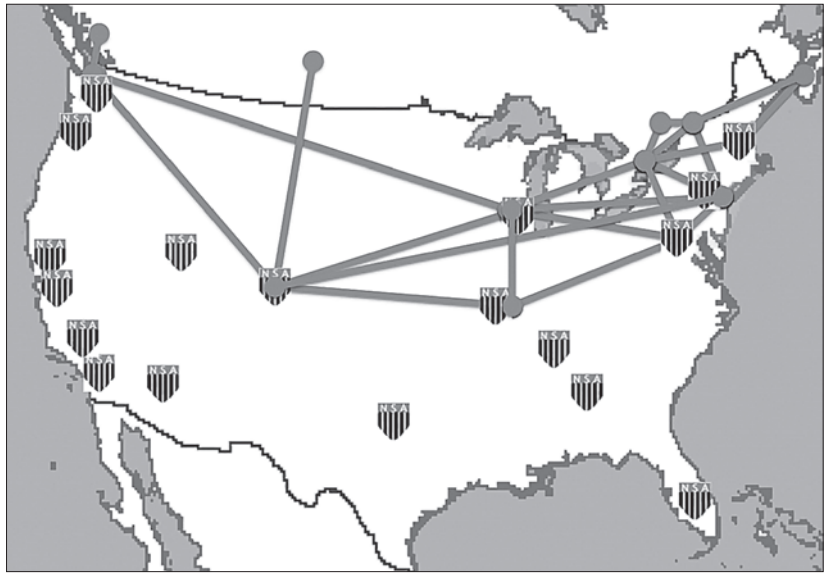
We have documented numerous cases where those accessing the websites of federal departments or agencies from within Canada would have their personal data routed via the United States. Even accessing the main Government of Canada site (canada.gc.ca) will involve boomerang routing for significant numbers of Canadians. Table 1 shows a sample of other examples, selected from the IXmaps database. Figure 4 shows a map produced by IXmaps, displaying the routes between users located in Canada and various federal government sites. One can easily imagine scenarios in which a Canadian would regard the information communicated to any one of these sites, or even the fact of a visit when viewed in the light of other online activities, highly sensitive and feel uncomfortable with this being available to the NSA or any other national security agency. As we will discuss more fully in the next section, unavoidable boomerang

routing to government sites also calls into question the government's ability to protect the integrity of its communications with citizens and undermines trust in vital governmental institutions.

Table 1: Selected Examples of Canadian Federal Department/ Agency/Office Websites Subject to Boomerang Routing

Federal Department/Agency/Office	Website
Canadian Air Transport Security Authority (CATSA)	www.catsa.gc.ca
Canadian Human Rights Tribunal	www.chrt-tcdp.gc.ca
Canadian Judicial Council	www.cjc-ccm.gc.ca
Citizenship and Immigration Canada	cic.gc.ca
Health Canada	www.hc-sc.gc.ca
Office of the Communications Security Establishment Commissioner	www.ocsec-bccst.gc.ca
Office of the Information Commissioner of Canada	www.oic-ci.gc.ca
Office of the Prime Minister	www.pm.gc.ca
Office of the Privacy Commissioner of Canada	www.priv.gc.ca
Parliament of Canada	www.parl.gc.ca
Privy Council Office	www.pco-bcp.gc.ca

Figure 4: A Selection of Canadian Boomerang Routes that Target Federal Government Sites



We've documented similar patterns of boomerang routing with provincial governments across the country. As the example depicted in Figure 3 illustrates, showing the route traffic follows between the University of Toronto and the Ontario Government, this boomerang pattern can even apply to Internet traffic between government institutions in the same province.

Table 2: Selected Examples of Commercial and other Websites Subject to Boomerang Routing

Banks	**Website**
Bank of Montreal	bmo.com
CIBC	cibc.com
Royal Bank	rbcroyalbank.com
Scotiabank	scotiabank.com
Toronto-Dominion	td.com
Universities	**Website**
Athabasca University	athabasca.ca
Dalhousie University	dal.ca
University of New Brunswick	unb.ca
University of Windsor	uwindsor.ca
York University	yorku.ca
Other Organizations	**Website**
Action Re-Buts	actionrebuts.org
Bell Canada	bell.ca
CPP Investment Board	cppib.com
Centre for Women in Business	centreforwomeninbusiness.ca
Dr. Tax	drtax.ca
Montreal Planetarium	espacepourlavie.ca
National Ballet of Canada	national.ballet.ca
Ottawa Public Library	bibliootttawalibrary.ca
Royal Astronomical Society of Canada	rasc.ca
The Toronto Sun	torontosun.com
Vancouver Economic Commission	vancouvereconomic.com

Commercial transactions over the Internet with Canadian businesses will also be subject to boomerang routing depending on the particular combination of ISPs at the customer and business ends of the communication. Banking, for instance, which is rightly treated to especially

strong security measures, for many Canadians is routinely subject to boomerang routing and the attendant dragnet NSA surveillance. We have documented that for every one of the Big Five banks, which dominate Canadian banking — BMO, CIBC, RBC, Scotiabank, and TD — there will be some customers whose interactions from home with their bank's website may be subject to foreign surveillance. Similarly, the IXmaps database contains traceroutes originating in Canada and destined for a wide variety of Canadian universities and colleges showing a similar pattern of US routing. Communication with the sites of non-governmental organizations, commercial organizations, libraries, media outlets, and cultural organizations have all shown evidence of boomerang routing. As Table 2 suggests, accessing any website, no matter the content or the context, could result in a boomerang route. A bank transaction, university research discussion, donation to a cultural organization, non-profit or advocacy campaign, tax software purchase, video view on a media outlet's site, and even library book check-out are all online activities that could involve a boomerang transmission path and consequent NSA surveillance.

Third Country Boomerang Routing

It is also worth noting that much of Canadian international Internet communications with countries other than the United States show 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. In this case, an obvious explanation is the location of transoceanic fibre optic cables and their landing points. As shown in the Telegeography's Authoritative Submarine Cable Map,[28] there are only two transatlantic fibre optic cables landing on Canada's East Coast (Hibernia Atlantic), compared with twelve landing in the United States. There are no trans-Pacific fibre optic cables landing on Canada's West Coast, whereas thirteen land in the United States.[29]

So far we have argued that the highly concentrated character of Internet interconnection has enabled the NSA to intercept nearly all traffic within and passing through the United States. Due to geographic factors, but also to the business relations among Canadian ISPs, a significant portion of Canadian domestic as well as third country international Internet communication boomerangs through the United States, and therefore is subject to mass NSA surveillance. We turn now to consider the policy implications of these routing and surveillance practices.

Policy Issues with Boomerang Routing

The controversies over the NSA's surveillance activities provoked by the Snowden revelations have focused on several recurring issues, both within the United States and internationally. The threats to personal privacy as well as other civil liberties and the challenges to national sovereignty are the two we address most directly here. Our emphasis on boomerang routing leads us also to consider the policy issues around the economic implications for Canada, which, while not immediately linked to state surveillance practices, promise to be a crucial factor in the remedial responses we'll discuss in the following section.

Privacy

Personal privacy is the issue that springs immediately to mind when discussing surveillance of any kind. However, we need to be cautious about the often unquestioned assumption that all surveillance represents an unavoidable threat to privacy, freedom of expression, and other important civil liberties.

This chapter, drawing on surveillance studies perspectives,[30] views NSA interception not as an isolated occurrence, but as reflecting a wider societal phenomenon, in which surveillance, "monitoring people in order to regulate or govern their behaviour,"[31] is a central organizing principle. Surveillance is often benign, even essential, but is becoming so pervasive and inextricably connected to everyday activities that we can characterize our contemporary Western life as a surveillance society. At the same time, it is important to recognize that notwithstanding its burgeoning extent and intensity, surveillance and its effects are not uniform, affecting everybody, everywhere in the similar ways.

Surveillance becomes a malign threat to civil liberties when it is conducted in a way that violates the democratic norms that govern potentially intrusive measures by the state. In Canada, the Supreme Court articulated these norms in 1986 when it developed the now widely recognized Oakes Test, based on *R. v. Oakes*.[32] Federal and provincial privacy commissioners have adapted and repeatedly applied this case in privacy contexts, assessing four key criteria: Necessity, Effectiveness, Minimality, and Proportionality. Suspicionless mass interception of personal communications would appear to fail this constitutional test on every count.

What makes the NSA surveillance especially problematic from a Canadian perspective is that foreigners' data under US jurisdiction is protected only through the definition of "foreign intelligence information," which is notoriously elastic. Notwithstanding Canada/US data sharing agreements and opinions of the federal and Ontario privacy commissioners prior to the Snowden revelations, there are strong legal arguments for the view that the level of privacy protection of Canadians' personal information in the United States is not equivalent to that at home. Once the data flows beyond the border, it no longer enjoys Canadian constitutional and other legal safeguards.[33] This means the NSA or other US agencies can legally intercept and analyze it without warrants or other judicial oversight. Furthermore, Canadians have no legal basis to challenge or remedy any abuses.

Network Sovereignty

When foreign governments or private actors play such central roles in a nation's critical communication infrastructure that they can conduct with impunity mass surveillance of domestic Internet traffic, as the NSA has the capability to do, it is not just privacy and other civil liberties that are threatened — national sovereignty is also at stake. It is useful in this context to employ the concept of "network sovereignty," which refers to an authoritative quality or process whereby an entity or set of entities distinguishes the boundaries of a network and then exercises a sovereign will or control within and at those boundaries. The sovereign can control any number of the components specific to the network, including its structural design, its evolution, development, and operation, and the extent to which the network operates, in whole or in part, and at what speed and capacity. Sovereignty can also be measured in terms of the relative level of control over the flow of content made possible by the network.

Though a new term, network sovereignty is far from a new concept. Any controlling entity, from a feudal monarch to an elected government, exercises a form of network sovereignty when it constructs any number of network systems ranging from transportation (e.g., roads, railroads, highways), utilities (e.g., water, electric) to communication (e.g., mail routes, telecommunication). As sovereigns, they can decide where these networks go, who or what can travel on them, and at what price.

The Canadian government exercises network sovereignty to serve national purposes in a variety of contexts. The dozens of laws

administered by Transport Canada[34] represent one example of the government's attempt to control Canadian transportation networks. For many years, network sovereignty has also been a focus of the Canadian media and telecommunications industry. Even before the Massey Commission of 1948 — which labelled the American media system an imminent threat to the maintenance of Canadian nationalism[35] — the notion that Canadian communication companies should remain in the hands of Canadians, and that those companies should be devoted to the maintenance of a national culture, were set as the primary goals of the Canadian communication system.[36] In the 1920s, when US-based radio stations were sending their signals well beyond the border, Canadian radio entrepreneur Graham Spry visited the US National Broadcasting Company for the purpose of studying their methods. While in New York, he learned of NBC's plan to "cover" Canada as "part of the North American radio orbit."[37] Speaking about the future of the Canadian broadcasting industry, he remarked famously, "It is a choice between the State and the United States."[38] Indeed, the concern that the United States could "cover" Canada in a grid of surveillance suggests that perhaps Spry's words are just as relevant now as they were almost one hundred years ago.

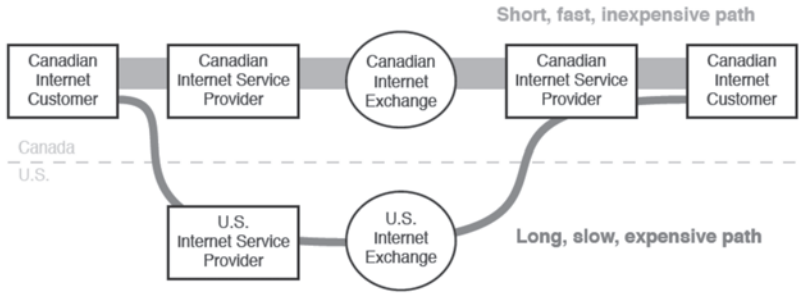
Following the long history of protectionist communication policy, the Canadian *Telecommunications Act* of 1993, still in effect to this day, already mandates Canadian Internet network sovereignty. The connection between the national telecommunications system, national sovereignty, and individual privacy is clear. The act states, "telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty."[39] Among the various objectives of the Canadian telecommunication system, the act stipulates that the system is "to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions."[40] Furthermore, the system has as a primary objective "to contribute to the protection of the privacy of persons."[41]

The boomerang routing identified by the IXmaps project, and the resulting threat of NSA surveillance, suggests that many of the ISPs operating in Canada are at odds with the law by jeopardizing both the sovereignty and privacy of Canadians mandated by the *Telecommunications Act*.

Technical and Economic Inefficiency

The widespread boomerang routing we have discussed here raises serious policy issues not only for those concerned for Canadians' privacy and sovereignty, but also for those seeking primarily to advance the vitality of Canada's Internet industry and infrastructure more generally. In particular, the Canadian Internet Registration Authority (CIRA), whose mission is 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,"[42] is concerned that dependence on US 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, the 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 latter. See Figure 5.

Figure 5: Boomerang Routing from an Efficiency Perspective



Source: Woodcock & Edelman, 2012

The CIRA's report concluded that

> Canadian Internet access is heavily and unnecessarily dependent upon foreign infrastructure, especially U.S. infrastructure. This dependence imposes significant burdens on Canadian Internet users:
>
> — Service prices are higher…[and] network speed is slower than would be the case if Canadian networks more densely interconnected domestically

> — When data en route from one Canadian network to another passes through other countries, the data is subject to examinations by companies and government authorities in those companies. Canadian data-protection laws are understood not to protect data as it passes through other countries.[43]

Explicitly linking economic and civil liberties concerns over boomerang routing in this way opens up important possibilities for the policy responses that we turn to next.

Policy Responses: Keeping Canadian Data within Canada

The most obvious way to keep Canadian data away from NSA interception is by routing domestic Internet traffic through Canada. While fully achieving this would be impractical, and clearly wouldn't address the problems of Canada's own mass state surveillance (e.g. Pugliese, 12 Oct 2009), much can be accomplished by taking the first, relatively easy steps in this direction. This would involve a combination of interrelated, infrastructural, administrative and legal developments. We consider each of these policy measures in turn, concluding with broader calls for a strong international regime of protection for Internet freedom which includes changes in best practices that encourage greater transparency by telecom carriers about their routing policies and practices that present surveillance risks.

Invest in Canadian Internet Infrastructure

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, public Internet exchange points, where all carriers can freely hand traffic off to each other, as well as the high capacity fibre optic trunk lines that connect them. The former are vital, as they enable the various local networks, such as retail ISPs and institutional networks, to reach communicants on other networks without having to depend on buying transit services from foreign carriers.

The CIRA has taken the lead in this approach by acting as a catalyst for the development of more Internet Exchange Points (IXPs) across Canada. As noted above, it is pursuing this strategy to address

economic and privacy issues. More specifically, CIRA's report summarizes the key benefits of this approach, including "reduc[ing] networks operational costs,…increasing the amount of bandwidth available to Canadian users,…reducing the risk of Canadian data becoming subject to foreign laws and practices,…improving the reliability of Internet access in Canada and its resilience to disaster and attack.[44]

CIRA observes that Canada is far behind other countries in developing IXPs, and that "IXPs typically cost less than $100,000 to establish, and return on investment can be seen in as little as a few days."[45] In 2012, the United States had eighty-five, whereas Canada had just two — OttIX in Ottawa and TorIX in Toronto. CIRA subsequently mounted a program to promote Canadian public IXPs and, by March 2015, had helped open three more — Montreal, Halifax, and Calgary.[46] A further five are identified as high-priority and fifteen as medium-priority.

Opening up access to trans-Canadian Internet backbone capacity, especially for linking these public IXPs, would also help avoid boomerang routing. The topic of Internet capacity and congestion is controversial and hampered by a lack of accurate public reporting on infrastructural capabilities and performance, in part because this information is treated as propriety competitive information.[47] In contrast to the need for financial investment and physical construction in the case of developing more IXPs, expanding effective long-haul backbone capacity for avoiding US routing may be more a matter of obtaining access rights to existing dark fibre than it is in laying more of it.[48] Should public funds be required, these appear to be available if there was a change in priorities. In sharp contrast to the many hundreds of millions of dollars the federal government has, appropriately, invested in extending Internet services to rural and remote areas over the past decade,[49] no comparable financial commitments have been made to ensuring that Canada's shared Internet backbone well serves the public interest.

Another form of investment that would help protect privacy is to enhance the security features of network infrastructure and operations to make mass suspicionless surveillance much more difficult. Most prominent in cybersecurity discussions, especially following the Snowden revelations, is to make end-to-end encryption a standard feature of Internet transmission. A substantive discussion of the pros and cons of encryption as a remedy for surveillance is beyond

the scope of this chapter, but a few observations are pertinent. As the Snowden documents reveal, as well as the demonstrated ability of Snowden himself to have escaped notice by the NSA when communicating with journalists, there are encryption tools, notably TAILS and ToR, that when used properly do provide effective protection against government spying. However, these techniques currently demand a level of technical sophistication and discipline that are well beyond the abilities of most people to use reliably and safely. It would take years of concerted development work to ensure the wide availability of a privacy protective communication infrastructure secured through encryption.

While the development of reliable and easy to use encryption techniques is highly valuable and even necessary, they alone would not be sufficient to adequately address the threat of unfettered surveillance by security agencies. The NSA and its Five Eyes partners have proven to be adept in finding a variety of ways of defeating security based on encryption — from gaining the cooperation of large Internet service providers (e.g., Microsoft) simply to hand over encryption keys, to breaking into the networks of reluctant vendors to steal them in bulk (e.g., Gemalto), to weakening the encryption standards themselves so messages can be cracked more easily. A vivid example of this is the NSA's BULLRUN program, a $250-million-per-year effort that sought to "insert vulnerabilities into commercial encryption systems."[50] In light of the inadequacies of encryption as an effective security measure for population-wide communication, at least in the foreseeable future, keeping data away from the major sites of Internet interception would be a significant and worthwhile achievement.

Public Procurement Policies to Give Greater Priority to All-Canadian Routing and Privacy Protection

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 will not guarantee that result, especially given the oligopolistic character of Internet transit practices. The purchasing power of public institutions, when deployed to further public interest goals, offers another legitimate and potentially powerful means to encourage domestic routing when contracting for Internet services. Government procurement policies are already well-established and

include various strictures designed to advance societal interests. In particular, the federal government's policy on contracting states the intention to "support long-term industrial and regional development and other appropriate national objectives."[51] An example of this in relation to the local storage of data can be seen in the Canadian government's current development of a cloud computing strategy. One of the proposed contract clauses, terms and conditions states that "The Services Provider (the Contractor) must not store any non-public, personal or sensitive data and information outside of Canada. This includes backup data and disaster recovery locations" (p. 27). It further considers the requirement "that all domestic data traffic be routed exclusively through Canada." (p. 8)[52] In a similar vein, a general procurement requirement that contractors providing Internet routing services peer openly at Canadian Internet points would "repatriate" a significant portion of traffic that currently travels via the United States. For example, if the Ontario government adopted this procurement requirement, and insisted that its Toronto ISPs peered openly at TorIX, we would not see the peculiar New York/Chicago boomerang shown in Figure 3, just to cross Queen's Park Circle. 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.

The policy measures considered so far, of pro-IXP infrastructural development and procurement requirements, promise a variety of financial and other benefits, thereby helping align a diverse array of actors potentially supportive of intra-Canadian domestic Internet routing. To target more directly the privacy risks of boomerang routing, we turn to Canadian data protection law.

Insist on Comparable Levels of Privacy Protection for Canadian Data Routed through Other Jurisdictions

Under existing Canada privacy laws, notably the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as various public sector laws, there is already a requirement 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 largely unfettered access to foreigners' data passing through the

United States, strongly suggests that Canadian carriers that route domestic Internet traffic via the United States or even simply hand data over to US companies inside Canada for domestic delivery, are not on the face of it in compliance with Canadian law. However, this is not a well-recognized fact. Part of the difficulty is that, prior to the Snowden revelations, some commissioners have ruled that notwithstanding the broad and intrusive powers of the *Patriot Act*, the fact of data falling under US jurisdiction, especially when considered in light of Canada/US data-sharing agreements, does not in itself constitute a violation of the "comparability" standard, as the service contracts might contain adequate protective provisions.[53] While it is highly unlikely that such contracts are strong enough to withstand the formidable powers of US security agencies, an in-depth assessment would require examining the contractual provisions of the third-party access in each case. This is effectively stymied by the unwillingness of service providers to divulge these contracts, which are typically covered by non-disclosure agreements.

This situation draws attention to the need for two important privacy policy initiatives: revisiting the issue of "comparable" protection in light of the Snowden revelations, and requiring more proactive disclosure by Internet service providers of the terms of data agreements between contracting parties.[54]

Partly in response to ambiguities about the threats posed to personal information in the wake of 9/11 and the *Patriot Act*, two provinces, Nova Scotia and British Columbia, updated their privacy laws to explicitly require that public bodies ensure that the personal information they hold is stored and accessed only in Canada.[55] While these laws help clarify the need for Canadians' data to remain under Canadian jurisdiction for protection, they appear premised on the conventional database model of information handling, with its emphasis on storage and access, and do not address the need for protection while in transit. This may be because at the time of enactment, the possibility of interception on-the-fly and the NSA's surveillance operations using splitters at Internet gateways were not part of the discussion. This suggests the need to include consideration of routing paths, along with storage location, when assessing privacy risks and possible legal protections.

It is important to note that while the focus of this chapter is on surveillance of Internet boomerang routing, reducing NSA interception only addresses one of several layers of the current

surveillance challenge facing Canadians. It is now well-documented that Canada's own signals intelligence agency, Communication Security Establishment (CSE) is involved in a variety of domestic surveillance activities.[56] This includes the potential interception of millions of Canadian Internet transmissions daily either via direct capture of the transmissions themselves, or through relationships developed with Internet carriers.[57] The Canadian government has also been attempting for years to expand the surveillance capabilities of federal agencies, and has recently been succeeding in the face of strong public opposition.[58] This domestic surveillance raises a host of privacy and other civil liberties concerns that are addressed in other parts of this book. Among them is the possibility that Canada/US data-sharing agreements may allow the NSA to circumvent the cross-border data routing debate entirely. But formidable as the challenges are to achieving surveillance reform within Canada, it remains the case that Canadians' data enjoy much better legal protection at home, with the prospects of protection from surveillance abroad much more remote. Advancing Canadian network sovereignty within a democratic framework will contribute to a broader movement to protect the privacy of Canadians from surveillance (foreign and domestic) in all its forms.

Conclusion

This chapter has examined the threats to Canadians' privacy, civil liberties, and national sovereignty posed by mass NSA surveillance of Canadian domestic Internet traffic. Drawing on IXmaps research project findings, we have demonstrated that a significant portion of this domestic Internet traffic transits the United States through prominent "choke point" sites of Internet backbone routing and NSA interception.

To address these threats, we propose an integrated set of policy responses involving infrastructural development, public procurement requirements, and stronger regulatory enforcement aimed principally at keeping Canadian data home. In pursuit of this goal, we propose

1. developing and promoting the use of Canadian public Internet exchange points (IXPs), in keeping with CIRA's initiative already underway;

2. opening access to Canada's long-haul Internet backbone, especially to facilitate traffic between public IXPs;
3. requiring Internet service providers in contracts with public bodies to include open peering at public Internet exchange points where these are available;
4. re-examining, in light of the Snowden revelations, the issue of comparable privacy protection for Canadians, personal data when exposed to US jurisdiction;
5. requiring greater transparency and accountability on the part of Canadian telecom carriers in terms of their internetwork routing practices, long-haul carriage capacity and utilization, and data-protection provisions in the contractual arrangements with transit providers.

Pursuing these measures implicates a range of public policy actors: Canadian Internet Registration Authority (1), Canadian Radio-television and Telecommunications Commission (1, 2, 4, 5), Industry Canada (1, 2), Privacy Commissioners (4, 5), and Treasury Board (3).

These measures are consistent with Canada's history of nation building through exercising and advancing network sovereignty in the face of the longstanding challenge of living peacefully but independently alongside the world's only remaining super power. We further argue that these measures are 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 that Snowden has revealed. To begin with, they do not tackle the NSA's surveillance programs, such as PRISM, that through partnerships with major online service providers popular with Canadians, notably Google, Facebook, Microsoft, Yahoo, Twitter, and Apple, 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 resolving the thorny issues around Canada's own suspicionless mass surveillance program that others in this volume discuss in more detail.[59] 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 and global Internet communication. This will require developing a robust international regime for protecting online privacy, free expression, and the other civil liberties that are the hallmark of democratic societies. Any efforts directed at better securing such public interests on a national scale should not interfere, but rather facilitate, achieving this transcendent goal. The policy responses outlined above are designed to accomplish this. Asserting national network sovereignty transparently and accountably in the pursuit of democratic ideals arguably provides one of the best bases for achieving similar ideals at a global scale. Pursuing the policy measures here can provide a valuable impetus in the global Internet governance enterprise by raising awareness of the issues at stake with boomerang routing, helping people understand better the hitherto murky but vital routing activities at the core of the Internet, and demonstrating that effective action can be taken to mitigate the menace of mass Internet surveillance.

Acknowledgements

The data reported in this chapter was generated through the IXmaps research project. We particularly appreciate the contributions of Antonio Gamba and Colin McCann. The project has been supported since 2009 by the Social Sciences and Humanities Research Council, the Office of the Privacy Commissioner of Canada and the Canadian Internet Registration Authority (CIRA). For more details, see IXmaps.ca

Notes

1. This chapter is a substantially revised and updated version of two previously published conference papers: Andrew Clement, "NSA Surveillance: Exploring the Geographies of Internet Interception," in *Proceedings on the iConference2014*, Berlin, 4–7 March 2014, and Andrew Clement, "IXmaps: Tracking Your Personal Data through the NSA's Warrantless Wiretapping Sites," 2013 *IEEE International Symposium on Technology and Society (ISTAS)*, Toronto, 27–29 June 2013, at 216, *IEEE-Explore Digital Library*, doi:10.1109/ISTAS.2013.6613122.

2. For a comprehensive, searchable collection of the documents Edward Snowden leaked and subsequently published by new media, see the Snowden Archive at <https://snowdenarchive.cjfe.org>.
3. James Bamford, *The Shadow Factory: The Ultra Secret NSA from 9/11 to the Eavesdropping on America.* (New York: Doubleday, 2008).
4. Andrew Clement, "NSA Surveillance: Exploring the Geographies of Internet Interception," in *Proceedings on the iConference2014*, Berlin, 4–7 March 2014.
5. *Washington Post*, "NSA Slides Explain the PRISM Data-Collection Program," 6 June 2013, updated 10 July 2013, <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.
6. James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*. (Boston: Houghton Mifflin, 1982); Bamford supra note 2; Mark Klein, *Wiring up the Big Brother Machine… and Fighting It* (Charleston, SC: BookSurge, 2009); Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2011).
7. Also referred to as "tromboning."
8. Jonathan A. Obar & Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty," in TEM 2013: *Proceedings of the Technology & Emerging Media Track – Annual conference of the Canadian Communication Association*, eds. P. Ross & J. Shtern (Victoria, 5–7 June, 2012), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792>.
9. IXmaps research project, see <http://ixmaps.ca>.
10. Ellen Nakashima & Joby Warrick, "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,' Observers Say," *Washington Post*, 14 July 2013, <http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html>.
11. Barton Gellman & Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, 6 June 2013, <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.
12. Andrew Blum, *Tubes: A Journey to the Center of the Internet*. (New York, Ecco, 2012).
13. J. Risen & E. Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, 16 December 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1145419200&en=87817a067833b164&ei=5070>.
14. Klein, *supra* note 5.
15. While the Bush administration initially denied the role of telecommunications carriers, it subsequently confirmed this in general terms.

Eric Lichtblau, "Role of Telecom Firms in Wiretaps Is Confirmed," *New York Times*, 24 August 2007, <http://www.nytimes.com/2007/08/24/washington/24nsa.html?ex=1345608000&en=4e8428cf3d46306c&ei=5090&partner=rssuserland&emc=rss>.

16. James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, 15 March 2012, <http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1>.
17. P. Harris, "US Data Whistleblower: 'It's a Violation of Everybody's Constitutional Rights,'" *The Guardian*, 15 September 2013, <http://www.guardian.co.uk/technology/2012/sep/15/data-whistleblower-constitutional-rights>.
18. Klein, *supra* note 5.
19. PBS Frontline, "Spying on the Home Front," 15 May 2007, <http://www.pbs.org/wgbh/pages/frontline/homefront/view/>.
20. For details of ratings and calculations see: <https://docs.google.com/spreadsheets/d/1x6aYnGmbQKzZGLUkWC4mX5eSRlDWpVKls_DjI_gV69A/edit?hl=en_US&authkey=CMeo8ZkG#gid=0>, accessed 5 May 2015.
21. See *Wikipedia*, s.v. "Traceroute," accessed 5 May 2015, <http:/en.wikipedia.org/wiki/Traceroute>.
22. Biases in the sample of traceroutes contributed by users to the database mean that this particular list of cities and the relative amount of domestic US traffic that could by intercepted by NSA splitters installed in them needs to be treated with caution. The chronic difficulties, widely recognized in the Internet routing research community, in accurately geolocating routers based on hostnames, IP addresses, and latencies, further complicate the picture. Nevertheless, we believe the overall conclusions about a relatively small number cities being sufficient to capture a very large proportion of US traffic remains valid. For more on these issues and the IXmaps project generally, see A. Clement, "IXmaps – Tracking Your Personal Data through the NSA's Warrantless Wiretapping Sites," *2013 IEEE International Symposium on Technology and Society (ISTAS)*, Toronto, 27–29 June 2013, <https://www.dropbox.com/s/9y4xtavova2qtj4/ISTAS13%20paper%2026%20IXmaps%20%E2%80%93%20Tracking%20May%2022.pdf>.
23. Andrew Clement, "IXmaps: Tracking Your Personal Data through the NSA's Warrantless Wiretapping Sites," 2013 *IEEE International Symposium on Technology and Society (ISTAS)*, Toronto, 27–29 June 2013, at 216, *IEEE-Explore Digital Library*, doi:10.1109/ISTAS.2013.6613122.
24. William B. Norton, *The Internet Peering Playbook: Connecting to the Core of the Internet* (N.p.: DrPeering Press, 2012).
25. See the Peers list at http://www.torix.ca/peers.php. As of 21 April 2014, Bell and Telus are not mentioned, and Rogers and Allstream peer only conditionally, but smaller ISPs such as Teksavvy and Distributel peer

openly (i.e., accept traffic for delivery without charge while expecting the same for delivery of their own traffic).

26. Some of the US network operators, such as Hurricane Electric, carry Canadian domestic traffic entirely within Canada, but nevertheless as mentioned later are still covered by US legal jurisdiction.
27. *Telecommunications Act*, S.C. 1993, c. 38, s. 7.
28. PriMetria, TeleGeography, last updated on 27 April 2015. (Washington, D.C.) <http://www.submarinecablemap.com/>, accessed 5 May 2015.
29. Data collected by IXmaps supports this pattern, in that there are currently ten times as many international traceroutes destined for a third country that are routed through the United States (130) as do not show US routing. However, these figures are not reliable, since we have so far made no systematic attempts to collect, geolocate, and analyze non–North American routes. It is also worth noting that even those international traceroutes that don't show a US-located router may be subject to NSA surveillance when passing through US-based gateways, or more clandestinely via submarine or landing point interception.
30. David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity Press, 2007).
31. J. Gilliom & T. Monahan, *SuperVision: An Introduction to the Surveillance Society* (Chicago: University of Chicago Press, 2013), at 2.
32. *R. v. Oakes*, [1986] 1 S.C.R. 103, <http://www.canlii.org/en/ca/scc/doc/1986/1986canlii46/1986canlii46.html>.
33. Austin, Chapter IV, this volume; Lisa Austin et al, "Our Data, Our Laws," *National Post*, 12 December 2013, <http://fullcomment.nationalpost.com/2013/12/12/our-data-our-laws/>. Similar principles apply even when data is handled in Canada by a US entity, such as the transit carriers mentioned above (e.g., Cogent, Level 3, Hurricane Electric), which are subject to US jurisdiction, notably to the *Patriot Act* (s. 215) and the *FISA Amendments Act* (s. 702).
34. Government of Canada, Transport Canada, *Acts and Regulations*, <http://www.tc.gc.ca/eng/acts-regulations/menu.htm>.
35. Mary Vipond, *The Mass Media in Canada*, 3rd ed. (Toronto: James Lorimer & Company), 2000.
36. Marc Raboy, *Missed Opportunities: The Story of Canada's Broadcasting Policy* (Montreal and Kingston: McGill-Queen's University Press, 1990); Standing Committee on Canadian Heritage, *Our Cultural Sovereignty: The Second Century of Canadian Broadcasting* (Ottawa: Parliament of Canada, June 2003), <http://cmte.parl.gc.ca/Content/HOC/committee/372/heri/reports/rp1032284/herirp02/herirp02--e.pdf>.
37. Cited in Raboy, *supra* note 34 at 23.
38. Raboy, *supra* note 34 at 40; Robert W. McChesney, *The 1997 Spry Memorial Lecture: The Mythology of Commercial Broadcasting and the Contemporary*

Crisis of Public Broadcasting (Montreal: 2 December 1997; Vancouver: 4 December 1997), <www.ratical.com/co-globalize/RMmythCB.pdf>.

39. *Ibid.* note 26, at 4.
40. *Ibid.*
41. *Ibid.*
42. Canadian Internet Registration Authority (CIRA), Mission Statement, <http://CIRA.ca>, accessed 2 March, 2015.
43. Bill Woodcock & Benjamin Edelman, *Toward Efficiencies in Canadian Internet Traffic Exchange, Canadian Internet Registration Authority* (September 2012), <http://cira.ca/sites/default/files/attachments/publications/toward-efficiencies-in-canadian-internet-traffic-exchange.pdff> at 1.
44. *Ibid.*
45. *Ibid.* at 2.
46. See CIRA Member News, "CIRA to Add Three More IXPs within Canada by 2015," 28 January 2013, <http://www.cira.ca/membership/enewsletters/vol-2-issue4/>.
47. Jesse Kline, "Why Canada Has 'Third World Access to the Internet,'" 24 September 2013, *National Post*, <http://fullcomment.nationalpost.com/2013/09/24/jesse-kline-why-canada-has-third-world-access-to-the-internet/>.
48. However, building greater trans-oceanic Internet backbone capacity for reaching other continents more directly and avoiding US transit, as Brazil is proposing, would involve considerable financial investment.
49. The federal government announced $305 million for rural high-speed Internet in its recent Canada 150 Digital Strategy. Canadian Press, "Ottawa's digital strategy targets privacy, rural internet: Long awaited 'Digital Canada 150' strategy unveiled by Industry Minister James Moore," *CBC News*, 4 April 2014, <http://www.cbc.ca/news/technology/ottawa-s-digital-strategy-targets-privacy-rural-Internet-1.2598097>.
50. James Ball, Julian Borger & Glenn Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian*, 6 September 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.
51. Treasury Board of Canada Secretariat, "Contracting Policy," Policy statement, last modified on 9 October 2013, <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=14494>.
52. Government of Canada, Canada's Cloud Consultation, Request for Information, Cloud Computing Solutions, EN578-151297/B, 2 December 2014 <https://buyandsell.gc.ca/cds/public/2014/12/02/272bfba752891ec35226f730cca2847e/ABES.PROD.PW_EEM.B033.E28243.EBSU000.PDF>, reported in Michael Geist, "Government's Cloud Computing Strategy Focused on Keeping Data in Canada," 30 January

2015, michaelgeist.ca (blog), <http://www.michaelgeist.ca/2015/01/governments-cloud-computing-strategy-focused-keeping-data-canada/>.

53. Ontario Information and Privacy Commissioner, *Reviewing the Licensing Automation System of the Ministry of Natural Resources, A Special Investigative Report*, [PC12-39], June 2012, <http://www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8933>.
54. Andrew Clement & Jonathan Obar, *Keeping Users in the Know or in the Dark: Data Privacy Transparency of Canadian Internet Service Providers*, IXmaps Research Report, 27 March 2014, <http://ixmaps.ca/transparency.php> also available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2491847>; Andrew Clement & Jonathan Obar, Keeping Users in the Know or in the Dark: 2014 *Report on Data Privacy Transparency of Canadian Internet Carriers*, IXmaps Research Report, 12 March 2015, <http://ixmaps.ca/transparency-2014.php>.
55. In the case of Nova Scotia, a new law was enacted — the Personal Information International Disclosure Protection Act SNS 2006, c.3., <http://nslegislature.ca/legc/statutes/persinfo.htm>.
56. See Ryan Gallagher & Glenn Greenwald, "Canada Casts Global Surveillance Dragnet over File Downloads," *The Intercept*, 28 January 2015, <https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/>.
57. Alex Boutilier, "Government Agencies Seek Telecom User Data at 'Jaw-Dropping' Rates," *Toronto Star*, 29 April 2014, <http://www.thestar.com/news/canada/2014/04/29/telecoms_refuse_say_how_often_they_hand_over_customers_data.html>; Amber Hildebrandt, Michael Pereira, & Dave Seglins, "CSE Tracks Millions of Downloads Daily: Snowden Documents," *CBC News*, 28 January 2015, <http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120>.
58. For instance, "lawful access" legislation, Bill C-13, *Protecting Canadians from Online Crime Act*, passed into law 20 October 2014. Other federal bills include: S-4, Digital Privacy Act, 2014; C-44, *Protection of Canada from Terrorists Act*, 2014, passed 2 February 2015; and C-51, *Anti-Terrorism Act*, 2015, passed the Commons 6 May 2015, after an unprecedented popular opposition campaign. See <https://stopc51.ca/>, accessed 6 May 2015.
59. See Austin, Chapter IV, and Parsons, Chapter IX.

References

Austin, Lisa M., Heather Black, Michael Geist, Avner Levin and Ian Kerr. (Dec. 12, 2013). "Our data, our laws," Opinion piece, *National Post*, http://fullcomment.nationalpost.com/2013/12/12/our-data-our-laws/.

Bamford, James. (1982). *The Puzzle Palace: A Report on America's Most Secret Agency*. Houghton Mifflin.

Bamford, James. (2008). *The Shadow Factory: The UltraSecret NSA from 9/11 to the Eavesdropping on America.* New York: Doubleday.

Bamford, James. (Mar. 15, 2012). "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)." *Wired*. http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

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

Clement, Andrew (2014). "NSA Surveillance: Exploring the geographies of Internet interception." *Proceedings on the iConference2014*, Berlin, March 4-7, 2014.

Clement, Andrew (2013). "IXmaps – Tracking your personal data through the NSA's warrantless wiretapping sites," *2013 IEEE International Symposium on Technology and Society (ISTAS)*, Toronto, June 27-29, 2013. 216 - 223. published in IEEE-Explore DOI: 10.1109/ISTAS.2013.6613122.

Clement, Andrew and Jonathan Obar (2014, March 27) *Keeping Users in the Know or in the Dark: Data privacy transparency of Canadian Internet service providers*, IXmaps research report. http://ixmaps.ca/transparency.php.

Clement, Andrew, and Obar, Jonathan (Mar. 12, 2015). Keeping Users in the Know or in the Dark: 2014 Report on Data privacy transparency of Canadian Internet carriers, IXmaps research report. http://ixmaps.ca/transparency-2014.php.

Dodge, M. and R. Kitchen (2002). "New Cartographies to Chart Cyberspace," *Geoinformatics* (April/May):1.

Electronic Frontier Foundation. (July 2, 2012). "Three NSA Whistleblowers Back EFF's Lawsuit Over Government's Massive Spying Program." https://www.eff.org/press/releases/three-nsa-whistleblowers-back-effs-lawsuit-over-governments-massive-spying-program.

Gallagher, Ryan and Glenn Greenwald. (Jan. 28, 2015). Canada casts global surveillance dragnet over file downloads. *The Intercept*. https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/.

Gilliom, J., and T. Monahan. (2013). *SuperVision: An Introduction to the Surveillance Society*. Chicago: University of Chicago Press.

Hildebrandt, Amber, Michael Pereira and Dave Seglins. (Jan. 28, 2015). CSE tracks millions of downloads daily: Snowden documents. *CBC News*. http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120

Katz-Bassett, E., J. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe. (2006, October). "Towards IP Geolocation Using Delay and Topology Measurements," in *ACM IMC '06*.

Klein, Mark. (2009). *Wiring up the Big Brother Machine… and fighting it*. Charleston, SC: BookSurge.

Landau, Susan. (2011). *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*. Cambridge MA: MIT Press.

Lyon, David. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

McChesney, Robert W. (1997). *The 1997 Spry Memorial Lecture: The mythology of commercial broadcasting and the contemporary crisis of public broadcasting*. (Dec. 2, 1997). www.ratical.com/co--globalize/RMmythCB.pdf

Norton, William B. (2012). The Internet Peering Playbook: Connecting to the Core of the Internet. (N.p.: DrPeering Press, http://drpeering.net/core/bookOutline.html.

Obar, Jonathan A. and Andrew Clement. (2013). "Internet surveillance and boomerang routing: A call for Canadian network sovereignty." In P. Ross & J. Shtern (eds.), *TEM 2013: Proceedings of the Technology & Emerging Media Track — Annual conference of the Canadian Communication Association*.

PBS Frontline. (May 15, 2007). "Spying on the Home Front." <http://www.pbs.org/wgbh/pages/frontline/homefront/view/>.

Pugliese, David. (Oct. 12, 2009). Canadian spies' 'Camelot': defence hoping to attract world-class talent with $880M intelligence complex. *National Post*. Retrieved July 26, 2013 from http://news.nationalpost.com/2012/10/08/canadian-spies-camelot-defence-hoping-to-attract-world-class-talent-with-880m-intelligence-complex/.

Raboy, Marc. (1990). *Missed opportunities: The story of Canada's broadcasting policy*. Montreal, QC: McGill–Queen's University Press.

The Standing Committee on Canadian Heritage. (2003). *Our cultural sovereignty: The second century of Canadian broadcasting*. Retrieved from http://cmte.parl.gc.ca/Content/HOC/committee/372/heri/reports/rp1032284/herirp02/herirp02--e.pdf.

Vipond, Mary. (2000). *The mass media in Canada* (3rd ed.). Toronto, ON: James Lorimer & Company.

Woodcock, Bill and Benjamin Edelman. (Sept. 2012) *Toward Efficiencies in Canadian Internet Traffic Exchange, Canadian Internet Registration Authority*, http://www.cira.ca/assets/Uploads/Toward-Efficiencies-in-Canadian-Internet-Traffic-Exchange2.pdf.