Addressing mass state surveillance through transparency and network sovereignty, within a framework of international human rights law – a Canadian perspective

Andrew Clement
Faculty of Information
University of Toronto
andrew.clement@utoronto.ca

A forthcoming paper to appear in the Chinese *Journal of Journalism and Communication Studies*.

December 13, 2016.

While comments and other feedback are most welcome, please do not cite without first contacting the author.

Abstract

Mass state surveillance of communications traffic on a global scale poses a significant challenge to internet governance efforts that seek to maintain consistency with well established human rights law. This paper identifies key features of the internet surveillance conducted by the Five Eyes security alliance and the threats these pose to privacy and other rights founded in multi-lateral legal agreements. Responding to these threats, a world-wide coalition of pro-privacy civil society organizations have developed a set of 13 Necessary and Proportionate Principles for evaluating surveillance legislation and practices. I highlight Principle #9 – Transparency, and show how through the development of an internet mapping platform, IXmaps.ca, it can be applied to making more visible the geographic specificities of internet routing, particularly where data travels and may be exposed to interception by surveillance facilities installed at major internet exchanges. As an internet policy transparency tool, IXmaps helps make visible the widespread phenomenon of 'boomerang' routing, in which communication that both originates and terminates in one country transits another. In the Canadian context, this means data traveling via the U.S. being exposed to NSA surveillance, while losing Canadian legal and constitutional protections. Furthermore, this tool reveals that most internet communications between Canada and a third country is routed through the U.S., facing similar interception risks. Both routing patterns pose a threat to privacy as well as 'network sovereignty,' treated as the ability of a nation to maintain effective control over vital aspects of its internet infrastructure and operations. When consistent with both international human rights law and the integrity of the internet as a unified open global communication medium, transparency and network sovereignty provide important principles of internet governance.

Table of Contents

Andrew C
Delete

Andrew C
Delete

Andrew C
Deleted

Andrew C
Deleted

Andrew C
Deleted

Introduction

The publication of documents provided by Edward Snowden to journalists in 2013 on the secret surveillance programs of the U.S. National Security Agency (NSA) and its signals intelligence partners in the other Five Eye countries (U.K., Canada, Australia and New Zealand) drew worldwide attention to the issue of mass state surveillance of internet communications. The breathtaking scope, scale and questionable legality of these surveillance programs have led many countries to re-assess the risks that such surveillance presents to the privacy of their citizens, as well as to their national sovereignty. Corporations seeking to shield their intellectual property and the personal information of their customers are re-considering the geographic location of their data centres as well as the routes data traveling between them follow. Civil society organizations concerned with human rights and internet governance have also begun formulating the principles upon which global communications should be regulated. The recent U.S. Presidential election has heightened the urgency of addressing these concerns.

This paper seeks to contribute to developing a global internet governance order that respects privacy and related democratic rights, within a framework of well established international human rights law. It also proposes an approach to internet governance

research that draws on transparency tools for probing critical aspects of internet infrastructure and operations to make them more publicly visible. The paper is written from the perspective of a Canadian researcher with longtime academic and advocacy interests in surveillance and privacy issues, especially as they are relevant to internet communications.[1] I have appreciated the many benefits of living in a liberal democracy, but have grown increasingly concerned that my government's security intelligence measures in response to 9/11 are not adequately effective or accountable, and are eroding the nation's fundamental espoused ideals. Canada's participation in the Five Eyes alliance, involving mass, untargeted surveillance at home and abroad, is particularly problematic. As a citizen, and especially one who enjoys the privileges of academic freedom and whose entire livelihood has relied upon the public purse, I bear a responsibility to publicly and constructively critique, in the areas of my competence, the Canadian government actions where they appear misguided.

I begin by sketching the most prominent Five Eyes mass state surveillance programs as revealed through the Snowden documents, highlighting the comprehensive scope of internet data collection as well as its physical and geographic specificities. This is followed by an overview of the various threats that such surveillance programs pose. I then summarize the *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance* report,[2] a remedial response developed collaboratively and endorsed by an international coalition of privacy-oriented human rights organizations. The next section elaborates on Transparency, one of the 13 Necessary and Proportionate principles that is especially pertinent for internet governance. Treating the IXmaps internet mapping platform as a transparency research tool, I highlight internet routing patterns revealing where and under what conditions personal data can be exposed to NSA interception. This supports a proposal for a specific form of network sovereignty, as another principle worth considering in the context of internet governance.[3]

Mass state surveillance

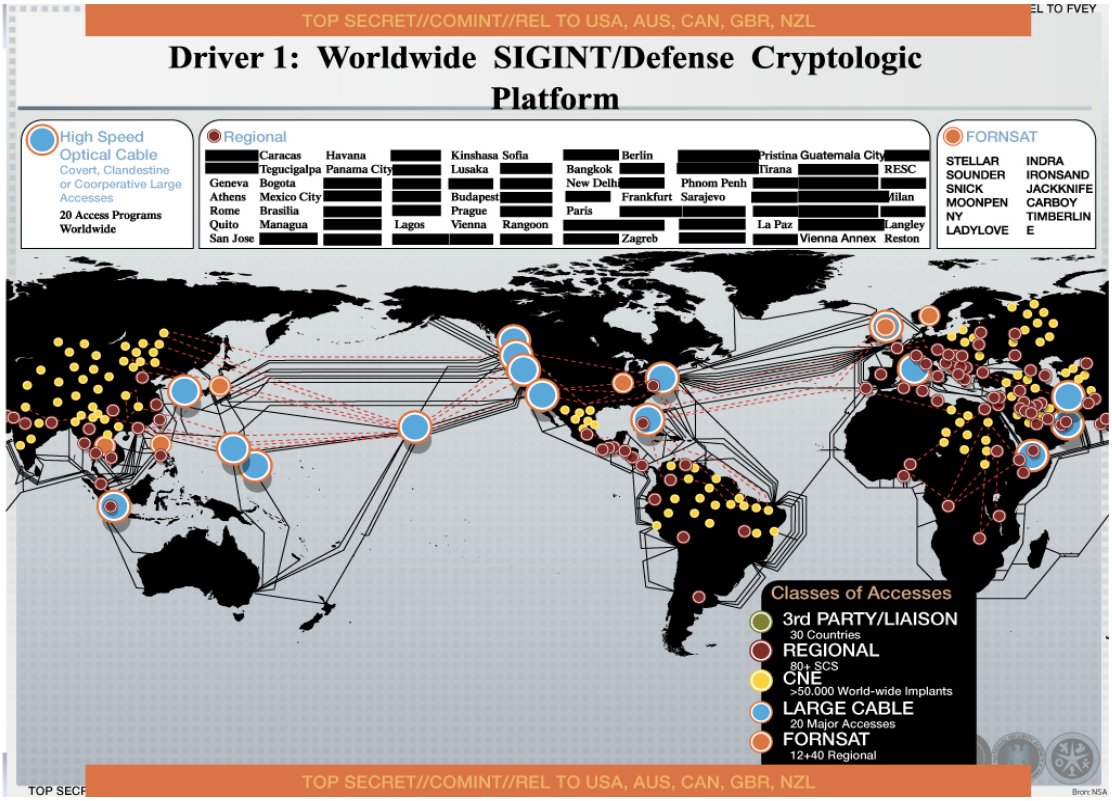
States have long spied on each other's communications, especially during times of war. The rise of radio communications in the late 19th century prompted states to begin developing the capacity for signals intelligence (SIGINT) – the interception, de-cryption and analysis of electronic signals for the purposes of informing action. Emerging from the Second World War, in which signals intelligence played a decisive role in the Allies victory, the intelligence agencies of the U.S., U.K., Canada, Australia and New Zealand formed the Five Eyes alliance to coordinate their surveillance efforts. While initially targeting the Soviet Union, even before the end of the Cold War the alliance, and the NSA in particular, had broadened the scope of its interception operations to include a wider range of targets. In the early 1980s, journalist James Bamford began his decades of investigative reporting on the NSA, drawing attention to the burgeoning capacity of the NSA to routinely capture massive amounts of personal information from both domestic and international communications.[4] After 9/11, the Bush Administration, in its pursuit of the 'War on Terror,' greatly accelerated these secret surveillance activities.

Five Eyes – "collect it all"

The first public indications of the expanded domestic spying program came in a 2005 *New York Times* report that President Bush had secretly authorized the NSA to eavesdrop on Americans' telephone and email communications to search for evidence of terrorist activity, but without the court-approved warrants ordinarily required for domestic spying.[5] However, the article provided little operational detail about what became known as the 'warrantless

wiretapping' program. Emboldened by the *Times* story, Mark Klein, a retired AT&T technician, disclosed that the NSA had secretly installed surveillance equipment in AT&T's main San Francisco internet exchange point, capable of copying and analyzing potentially all of the internet traffic passing through that location. But it wasn't until June 2013, when the *Guardian, Washington Post* and other major newspapers began publishing the secret documents provided by former NSA contractor Edward Snowden, that we learned for the first time details of the NSA's comprehensive array of data collection, archiving, mining, analysis and visualization programs. Over the subsequent months, Snowden's documents revealed that the Five Eyes alliance had successfully pursued a "collect it all" strategy,[6] building what it referred to as a "Worldwide defense/SIGINT cryptologic platform", i.e. a global signals intelligence infrastructure tapping into all the major communications pathways. See Figure 1.

Figure 1: Five Eyes global signals intelligence infrastructure[7]



While much of the public controversy that these revelations have provoked has focused, at least in the U.S., on whether collecting or accessing data about Americans is legal or even constitutional, of wider significance is the existence of a worldwide apparatus designed for and capable of intercepting virtually all electronic communications around the globe. This effectively implicates all major internet carriers and service providers, and hence nearly all internet users. Any internet governance scheme of global scope must grapple substantively with this new and disturbing reality.

Besides the extraordinary technical prowess that the U.S. is able to deploy in the service of its perceived surveillance and security needs, the U.S. also has a strategic geographic advantage in relation to international data flows. And the NSA is well aware of this. As Figure 2, one of the first Snowden documents to be published[8] indicates, a disproportionate amount of global

internet traffic is routed via the U.S., even when neither origin nor destination is in the US. Once on American soil, the NSA has several ways to access foreigners' data without legal restriction.

Figure 2: U.S. as World's Telecommunications Backbone[9]

PRISM - collect it from data servers

One way that the NSA takes advantage of its strategic location is through the PRISM program. This involves "tapping directly into the central servers of nine leading U.S. Internet companies."[10] Starting in 2007, the NSA has arranged for access to the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The *Washington Post* reports that the "NSA collects, identifies, sorts and stores at least 11 different types of electronic communications [including] Chats, E-mail, File transfers, Internet telephone [VoIP], Login/ID, Metadata, Photos, Social networking, Stored data, Video, Video conferencing."[11] PRISM appears to have arisen in response to both legal and political pressures after Klein's revelations brought the 'warrantless wiretapping' program to light, as well as in order to get around the increasing use of encryption that rendered analysis of message content intercepted in transit more difficult. Because the on-line services of these nine companies are popular globally, and are located on US territory and hence covered by US law which provides no protections to foreigners' data, their users outside the US can expect their personal data to be wide open to NSA inspection.

Upstream – collect it in transit

When the recent round of NSA surveillance revelations broke in June 2013, it was the PRISM and bulk telephony meta-data collection that garnered the greatest media attention. However, it is the NSA's suite of programs that intercept data in transit, known collectively

as Upstream, with an even wider reach than either of the other two, that are arguably the programs most challenging to human rights. A top secret training slide (see Figure 3), with a world map showing submarine traffic patterns as background, distinguishes between PRISM and Upstream, characterizing the latter as "Collection of communications on fiber cables and infrastructure as data flows past." As this quote suggests, there are several ways of accessing data networks. Easiest is installing 'splitters' within major internet switches of willing internet carriers such as AT&T, as Klein revealed. Where switch operators are not sufficiently cooperative, the NSA pursues more technically challenging methods of interception. One of these is to clandestinely implant spyware in the switches, routers or other network devices, which then quietly transmits data back to the NSA or aggressively attacks the local network. The NSA's Quantuminsert program automates this implantation process, providing the ability to infect millions of devices.[12] Another method is to tap into the cables at some point along the route between the switches. Since much of the international internet traffic travels by submarine fiber optic cable, this often means installing taps at landing stations or even mid-ocean.[13]

Figure 3: NSA training slide for PRISM program[14]

In all of these forms of interception, deep packet inspection (DPI) is used to examine and potentially store all aspects of the traffic, including meta-data (e.g. to: and from:) as well as communicative content.

In brief, these data collection activities of the NSA, together with its Five Eyes partners, can capture a very large proportion of internet communications world wide. In aggregate they produce staggering quantities of information. William Binney, a former NSA mathematician and Technical Director of the World Geopolitical and Military Analysis Reporting Group, estimated in 2012 that the agency had "assembled on the order of 20tn transactions about

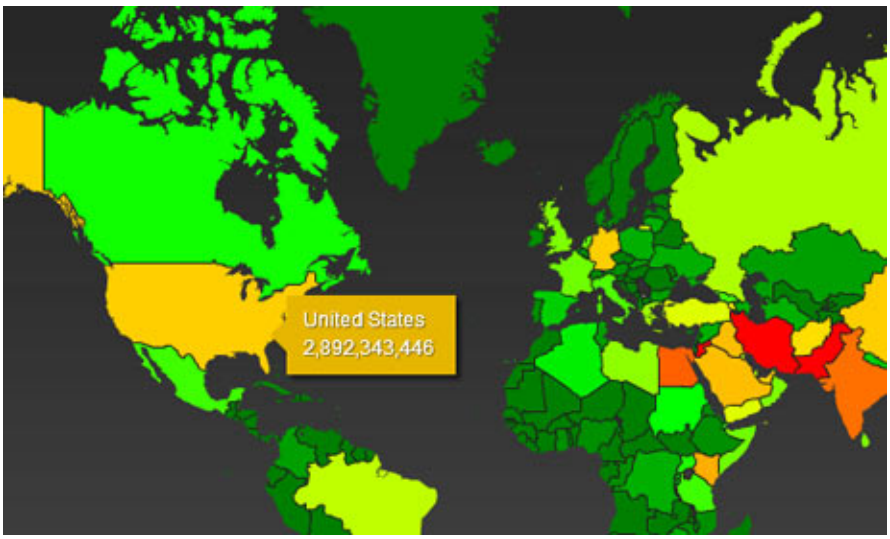
US citizens with other US citizens", and this included "only … phone calls and emails". In 2010, the Washington Post reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."[15]

Processing this information to produce intelligence presents a formidable challenge. Two analysis and visualization programs, *Boundless Informant* and *X-Keyscore*, give a broad overview of the scale and intensity of surveillance capability.

Boundless Informant – aptly named

The top secret, Boundless Informant program is a data mining tool described in an official Global Access Operations (GAO) FAQ, as providing "the ability to dynamically describe GAO's collection capabilities (through metadata record counts) with no human intervention and graphically display the information in map view, bar chart or simple table".[16] A GAO slide presentation claims the program uses 'Big Data technology to query SIGINT [signal intelligence] collection in the cloud to produce near real-time intelligence describing the agency's available SIGINT infrastructure and coverage."[17] While this aptly named tool doesn't access all of the information that the NSA collects (e.g. information covered by FISA restrictions is not included), the volume is impressive. The *Guardian* reports that "in March 2013 the agency collected 97bn pieces of intelligence from computer networks worldwide", including nearly 3bn in the U.S. The accompanying 'heat map,' showing relative amounts of data collected in various countries, indicates that the NSA collected similar quantities of data that month within Germany, Saudi Arabia, Iraq, Kenya and China, as they are all rendered in the same orange colour as the U.S. (See Figure 4). Overall, this map shows that interception is widespread around the globe.

Figure 4: Heat map of NSA meta data collection in March 2013[18]



X-KeyScore – Google for spies

X-KeyScore is a query tool designed to allow authorized analysts to interrogate the NSA's vast world-wide intelligence holdings through a desktop interface. 'Selectors', such as an email address or IP address, can be used to access stored data as well as initiate "ongoing 'real-time' interception of an individual's internet activity."[19] Due to the large volumes collected, data is initially held close to the point of capture and much of it is deleted after a few days.[20] Figure 5 shows the world-wide distribution of these caches, again demonstrating the broad geographic scope of NSA surveillance. It is not just NSA analysts who have access to this data, but as the top of the slide shows, the security agencies in the other "Five Eyes"

countries – Australia, Canada, Great Britain and New Zealand. There are also reports of access by intelligence services in other US allies such as Germany.[21]

Figure 5: Location of data caches accessible by X-Keyscore[22]

The discussion so far has focused exclusively on the Five Eyes surveillance. This is largely because, thanks to Snowden's whistleblowing, much more is known publicly about that than about internet surveillance by other countries. However, there is substantial evidence that signals intelligence agencies in many other countries also intercept internet communications, at least internally, for state security and other purposes. Reporters Without Borders, in its 2014 'Enemies of the Internet' report identifies 20 countries that conduct internet censorship and surveillance that pose threats to human rights.[23] Of these 20, and in addition to the Five Eyes countries on the list (US and UK), the larger ones such as China, India and Russia all also have the resources, skills and incentive to conduct internet surveillance beyond their borders. It would be surprising if these countries haven't bolstered their extra-territorial surveillance activities following the Snowden revelations, and are poised to do so again in the wake of the recent U.S. presidential election, putting Donald Trump in charge of the US military and its formidable surveillance apparatus.

What is wrong with mass state surveillance?

While state-based internet surveillance has legitimate purposes, and few would suggest that it be abolished entirely, the wide scope, fine granularity and questionable legality of the forms of surveillance just described pose many significant challenges to internet communications. Unregulated mass surveillance by state and corporate actors presents a serious threat to the openness, security, privacy, and diversity of communications that the internet relies on to thrive. When internet users, whether individuals, governments, corporations or civil society groups, cannot trust that their communications are not interfered with or won't be used against them, the internet's value, legitimacy and generativity are eroded. This will either push users to withdraw or to adopt counter measures that at the very least add friction, and worse invite an arms race of ever escalating surveillance measures and counter measures. Either way, mass surveillance detracts from the internet's potential as a universally accessible common resource and an open platform for socio-economic innovation. Left unfettered, mass internet surveillance effectively

poisons the well that we now all draw upon as an infrastructure vital for everyday living. It is therefore incompatible with one of internet governance's central missions – "to develop shared policies and standards that maintain the Internet's global interoperability for the public good."[24]

The 13 Necessary and Proportionate Principles – An international human rights law response

Even before the Snowden revelations, the expansion of state surveillance of internet communications, especially since 9/11, was becoming better known publically and raising alarm. In response to the threats that this posed to privacy in particular, an international coalition of human rights groups began a global consultation process to develop a framework to evaluate whether surveillance laws and practices were consistent with human rights. No states were targeted in particular, and there was recognition that some forms of secret surveillance may be necessary. The ambition was not to abolish communication surveillance entirely, but rather to bring it within internationally agreed legal norms designed to protect basic rights. The result was the publication in May 2014 of *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*.

As its Preamble notes, the 13 *Necessary and Proportionate (N&P) Principles* are based on treating privacy as a fundamental human right, one that is "essential to human dignity and reinforces other rights, such as freedom of expression and information, and freedom of association."[25] The right to privacy has been well recognized under international human rights law since the 1948 proclamation of the Universal Declaration of Human Rights. The right of everyone to the "protection of the law against … arbitrary interference with his [sic] privacy," is guaranteed in Article 12.[26] This is given legal status in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) that came into force as an international treaty in 1976.[27] 74 parties have signed, including all of the Five Eyes countries.

The 13 *Necessary and Proportionate Principles* are:

1. Legality
2. Legitimate aim
3. Necessity
4. Adequacy
5. Proportionality
6. Competent judicial authority
7. Due process
8. User notification
9. Transparency
10. Public oversight
11. Integrity of communications and systems
12. Safeguards for international cooperation
13. Safeguards against illegitimate access and right to effective remedy

The Scope of Application section of the *Necessary and Proportionate* report notes:

> The Principles and the Preamble are holistic and self-referential – each principle and the preamble should be read and interpreted as one part of a larger framework that, taken together, accomplish a singular goal: ensuring that laws, policies, and practices related to Communications Surveillance adhere to international human rights laws and standards and adequately protect individual human rights such as privacy and freedom of expression.

> These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance — including enforcing law, protecting national security, gathering intelligence, or another governmental function. They also apply both to the State's obligation to respect and fulfil individuals' human rights, and also to the obligation to protect individuals' human rights from abuse by non-State actors, including business enterprises.[28]

The *13 Principles* are aimed specifically at state actors, to provide a framework for evaluating whether their surveillance laws and practices are consistent with their obligations under international human rights law. However, given the global nature of the internet and the increasingly pervasive state surveillance embedded within it, these principles also provide a good foundation for developing internet governance norms more broadly.

The Transparency Principle

'Transparency, ' N&P Principle #9, is especially relevant to internet governance. Without a good understanding of what personal information is collected or accessed, by whom, for what purposes, with what consequences, under what legal authority, with what oversight, etc., individuals are poorly equipped to make adequately informed decisions either as internet users, e.g. about whether the privacy risks they face personally are acceptable, or as citizens, e.g. "when deliberating with others over matters of public policy."[29] Transparency, because it is a vital pre-condition for informed decision-making and organizational accountability, is widely recognized as a foundational human rights and democratic governance principle. Given the complexities and invisibilities inherent to networking technologies generally, compounded by the secrecy and controversy which surrounds internet surveillance in particular, appropriate transparency is both especially important as well as extraordinarily difficult to achieve in the internet governance context. Total transparency about all aspects of internet operations would be an impossible goal nor would it be desirable given various other legitimate concerns that would need to be balanced with it. As noted above, the 13 N&P Principles don't treat any one as pre-eminent. In particular, some prospective Transparency measures would need to be considered carefully in relation to Principle #11 - Integrity of communications and systems. Nevertheless, Transparency is sufficiently important that it should be treated as the default, with the onus on those who propose any restrictions on it to justify them in the service of upholding human rights.

Transparency is applicable to many facets of internet activity. The N&P description of the Transparency Principle focuses mainly on the reporting of requests made by state authorities, such as law enforcement agencies, to communications service providers for the personal information of individuals. It reads:

> States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for

> Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.[30]

Transparency reporting on access requests is an important area of current concern, but there are many other aspects of internet operations relevant to the intersection of human rights and internet governance. A key issue is what jurisdictions, and hence what laws, are applicable to internet communications. Without some form of proactive disclosure, this may be difficult to determine since internet routing, storage and guiding imaginaries famously pay little regard to political boundaries. Related to this is the ability to know where one's data may be subject to surveillance, and by which agents.

Transparency research into internet routing and state surveillance

A defining feature of democratic governance is the premise that those who are affected by particular policies or practices have the right to a voice in shaping them. When technologies play a central role in those policies and practices, this premise implies that those affected have a basic understanding of how the technologies in question work. Furthermore, whether treating privacy as the "right to be left alone" or, especially in the German constitutional sense as "informational self-determination,"[31] for people to protect their privacy while on-line they similarly need to know some internet basics, such as how their data is routed, where it travels and what risks it faces along the way. However, few people outside of the technically trained have an adequate understanding of these pertinent details. The popularity of the misleading imaginary of internet as a "cloud" further confounds insight into where one's internet data actually travels and who handles it along the way. A more apt metaphor in privacy and governance matters is that the internet is effectively an inscrutable 'black box' that needs to be opened up to public understanding. If internet governance is to conform with democratic norms, particularly in relation to privacy protection, it needs to pursue greater transparency about the routing of personal data, the jurisdictions involved, where data can be intercepted and those intermediaries who have responsibility for protecting this data.

A number of on-going research initiatives probing various aspects of internet operations can contribute to making them more transparent and provide the basis for more informed internet governance. These include: Cooperative Internet Association for Internet Data Analysis (CAIDA), Measurement Lab (M-Lab), RIPE Atlas, Packet Clearing House and PlanetLab to name only a few of the more prominent ones.[32] Generally speaking, these initiatives adopt a technical orientation, addressed to a professional audience. None address state surveillance or privacy issues directly.

IXmaps as an internet transparency tool

Building on and complementing these related internet transparency initiatives, the IXmaps project seeks to promote greater public understanding of internet operation and human rights risks by rendering more visible the typically hidden workings of the internet core. In particular, the IXmaps internet mapping platform as a transparency tool provides lay users with a means for probing, from their own perspective, hitherto obscure technical and institutional aspect of internet routing. It thus offers anyone a way to appreciate better how the 'cloud' is implicated in issues of physicality, geography, jurisdiction, governance, policy, human rights, and mass state surveillance. The IXmaps project shares with the other transparency initiatives mentioned above an interest in revealing hidden features of

internet structure and operation. IXmaps is distinctive, however, in its orientation to surveillance and privacy issues.

I co-launched the IXmaps.ca project[33] in 2009, mainly in response to Mark Klein's revelations of the NSA interception operations at 611 Folsom Street in San Francisco, AT&T's main regional switching centre. The original aim was to explore the feasibility of identifying whether one's personal internet traffic passed through this or other suspected NSA surveillance sites. Over subsequent years we have upgraded the platform in its traceroute generation, mapping and public pedagogical capabilities, to reach a wider audience.

In order to produce internet data that reflects individual users' on-line activity and preferences, as well as to involve them more directly in the public education aspects of its mission, IXmaps takes a crowd-sourced approach to generating the traceroute data that it requires for mapping internet routes. Traceroutes measure the route path of data traveling across the internet as a series of hops from one router to the next. We invite internet users, wherever they are located geographically, to contribute their own routes to our database and then check which ones pass through any of the suspected NSA interception sites. Individuals add their traceroutes to the IXmaps database by first installing a version of the common traceroute generation software we have customized and then running this program to initiate traceroutes to a variety of destination URLs of their choosing. We assign location information for each router encountered based on various IP address geolocation approximation techniques.[34] Users can then selectively map their own or others' traceroutes based on a Google Maps mashup. Traceroutes are rendered as coloured dots, representing the routers, and lines, representing the hops data takes from one router to the next. The colours of the dots and lines indicate the particular ISP or internet carrier. (See Figure 7 below for an example.) As of November 2016 the IXmaps database contained over 160,000 traceroutes, contributed by more than 600 submitters targeting approximately 4,000 distinct destination URLs. While most routes originated in Canada and the U.S., contributions have come from over 25 other countries worldwide.

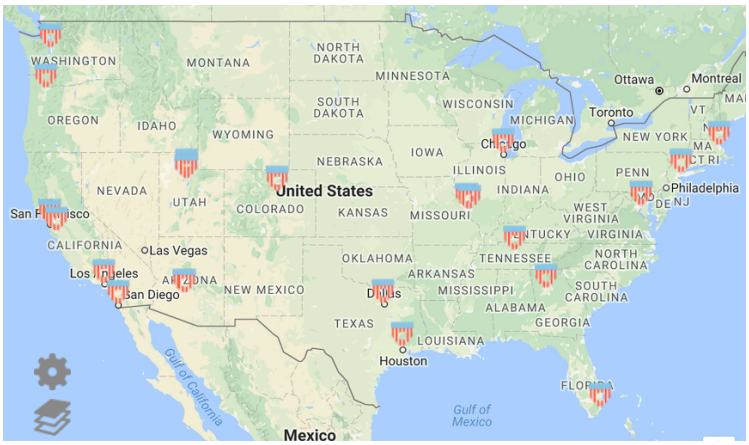
The IXmaps platform, with its extensive and growing database of user-generated traceroutes that record detailed information about the physical paths data takes across the internet, which ISPs carry this data, where they hand it off to other carriers as well as make it available for interception by surveillance agencies, offers a potentially powerful transparency research tool for investigating a range of internet governance issues. Here we'll focus on the issue that motivated its creation – making more visible the NSA's bulk interception of traffic within the U.S., and what this implies for Canadian domestic internet traffic as well as for global communications transiting the U.S.[35]

Mapping internet traffic through NSA surveillance 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.[36] However, these 6 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, estimates that AT&T had 15-20 splitter sites.[37] 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, we developed a crude schema for scoring cities based on how much internet traffic was likely to pass through them. Using only our personal rough estimates of 3 determinants of prominence of internet routing location, and crude relative weightings: existing telecom infrastructure (10); city size (population) (5); and geographic location in relation to major internet routes(4), we developed an ordered ranking of the US cities. We picked the 18 cities with highest aggregate scores as the most likely candidates for the NSA to install interception facilities. These are shown in Figure 6, an IXmaps screenshot, where the shield icons represent suspected NSA interception facilities. To test our hypothesis, we examined all the US-only routes in the IXmaps database, which currently numbers 7,263. Of these, 6,767 passed through at least one of the 18 cities we identified as sites where the NSA would find it most productive to capture internet traffic. In other words, installing splitters in the major internet exchange points in just these cities would be sufficient for the NSA to intercept 93% of our US only traceroutes![38]

Figure 6: 18 US cities most likely to host NSA splitters



[and a black and white version that may reproduce better.]

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 a powerful indication of the fact that, if the NSA install splitters in relatively few strategic internet choke points, it is technically feasible for it to intercept a very large proportion of U.S. internet traffic. This high percentage helps to justify our claim that these cities are strongly suspected of hosting

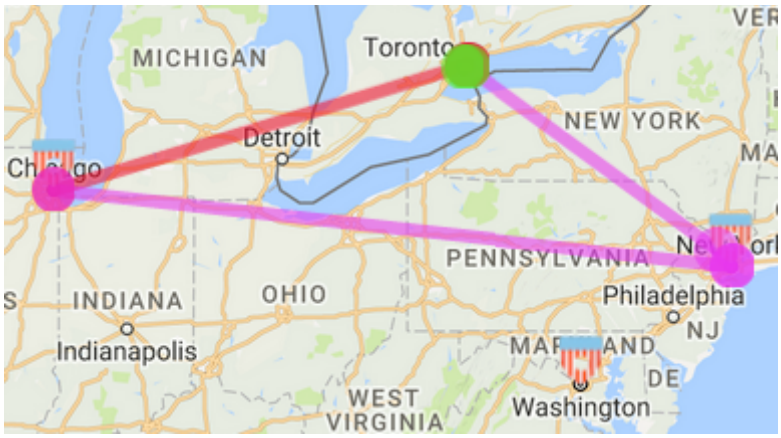
NSA warrantless surveillance facilities. Since we came up with this list of 18 prime NSA surveillance sites in the US, top secret NSA slide presentations released as part of the Snowden collection show a larger set of internet interception points within the U.S., including all of the cities we had identified.[39] This strongly suggests that the NSA has the capacity to capture nearly all US internet communication, including domestic traffic as well as that transiting through the US on its way to other destinations.

The fact that the heavy concentration of internet traffic flowing through a relatively small number of sites provides attractive opportunities for surreptitious interception applies globally as well. This is illustrated in Figure 1 above, with the large blue circles indicating 20 major access sites for intercepting traffic on transoceanic fibreoptic cables. This also vividly challenges the popular image of the internet as an ethereal, placeless 'cloud.' Quite the opposite. A relatively few key exchange points, housed in large buildings packed with routers linking high capacity trans-continental, trans-oceanic and regional fibreoptic cables with each other constitute the core components of today's internet. While serving a vital function in internet communication they also offer an attractive venue for mass state surveillance. Understanding better who does what with the data passing through these sites is crucial for achieving effective internet governance, as well as protecting human rights in our contemporary network society.

Same country 'boomerang' routing

So far we have concentrated on traffic that explicitly travels via US routing centres, either originating or terminating in the US, or both. As alluded to above and is well known in internet routing circles, traffic that neither originates nor terminates in the US may nevertheless transit via the US, mainly due to the interconnection arrangements of the major international carriers.[40] However, the extent of this practice and its surveillance implications are less well known. While this affects many countries, Canadian traffic in particular, due to its proximity to the US as well as the structure of the North American internet service industry, is especially prone to routing via the US. We refer to traffic that originates and terminates in the same country, but transits another, as "boomerang traffic." Currently the IXmaps database contains 29,963 routes with both ends in Canada. Of these 8,374 travel via the U.S., indicating that that approximately 28% of the Canadian routes follow a boomerang pattern. That long distance Canadian routes may be routed via the US is not surprising, but we were struck by the number of routes that start and end in the same Canadian city, but are also routed via the US. We have found over 270 such boomerang routes based in Toronto alone, representing 21% of such same city boomerangs. This is not far off the 28% figure for Canada as a whole, indicating that it is not routing efficiency alone that can account for this. Figure 7 shows an IXmaps screenshot of one such Toronto to Toronto boomerang route, traceroute #35080**,** which transits New York and Chicago, both cities strongly suspected of hosting NSA splitters. Whether crossing the continent, or returning to the same city, Canadian boomerang traffic is almost entirely exposed to NSA surveillance.

Figure 7: A Canadian boomerang route based in Toronto



[and a black and white version that may reproduce better.]

Third country 'boomerang' routing

It is also worth noting that much of Canadian international internet communications with countries other than the U.S. show similar 'boomerang' characteristics, in the sense that the traffic passes through the US, almost invariably via a city where the NSA has splitter interception facilities. The IXmaps database currently contains 7,233 routes that either originated in Canada and terminated outside both Canada and the US, or originated outside both Canada and the U.S. and terminated inside Canada. 81% of these third country routes transited the US. An obvious explanation for this is the location of transoceanic fibreoptic cables and their landing points. As shown in TeleGeography's authoritative Submarine Cable Map 2014,[41] there are only two trans-Atlantic fibreoptic cables landing on Canada's East Coast (Hibernia Atlantic), compared with 12 landing in the US. There are no trans-Pacific fibreoptic cables landing on Canada's West Coast, whereas 13 land in the US.[42]

As several NSA documents indicate (see Figure 1 above), Canada is not alone in depending on U.S. transit for internet communications with end points outside the U.S. IXmaps provides a useful glimpse into this phenomenon. Out of the 1,500 routes in the database that neither originate nor terminate in either Canada or the U.S., about one-third transit via the US.[43] That so much internet traffic relies on U.S. transit not only threatens the privacy and other rights of internet users, it also challenges the sovereignty of the nation states involved, in the sense that the integrity of the communication system that a state depends upon internally, as well as its ability to manage its bi- and multi-lateral relations with other

nation states, is compromised by dependence on a hegemonic power. I explore the implications of this next.

Network sovereignty – a Canadian perspective

The findings from the IXmaps research, that a significant portion of Canadian internet communications, domestic as well as with third countries, is exposed to NSA interception, has policy implications not just for Canada but for global internet governance more generally. States can pursue three broad approaches to address the threats that Five Eyes mass state surveillance pose:

1) Enabling strong data encryption by default so that when interception occurs it reveals little or nothing about the communication;
2) Routing traffic away from NSA interception points as an exercise of network sovereignty; and
3) Developing a strong international regime of internet regulation so that human rights are respected regardless of where data may travel.

Each of these approaches has their merits and ardent proponents, as well as their limitations. None alone offer an adequate solution in the near term, nor can any be dismissed at this point. Rather than being mutually exclusive, they are complementary and worth pursuing in parallel.

The first approach to protecting communications from surveillance, strong encryption by default, is vigorously pursued in the technology community, but faces resistance by many state agencies. End to end encryption offers protection against a wide variety of threats, not just that of mass state surveillance. It provides an essential technical foundation for preserving rights to privacy and anonymity, a point recognized in *Necessary and Proportionate* Principle #11 Integrity of communications and systems.[44] The report cites the UN Special Rapporteur on Freedom of Expression who noted in 2013:

> the security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption.[45]

Encryption as a means for protecting communications is a complex subject and beyond the scope of this paper to explore adequately. Suffice to say that it has a number of limitations as a way to protect human rights. Among the most significant are: encryption doesn't readily shield key metadata from capture (e.g. To: and From: addresses need to be sent in the clear for routing purposes); contemporary encryption tools often demand technical skills and disciplined application beyond the abilities of most internet users; and various encryption techniques may not be reliable, having been compromised by Five Eyes efforts to introduce 'backdoor' access. Exercising network sovereignty in terms of internet routing offers a complementary approach that addresses some of the inadequacies of encryption. It is the principal focus of this section.

Network sovereignty as data localization

Routing traffic away from NSA interception points offers states an obvious way of shielding their citizens' data from the threats of U.S. based state surveillance. In the case of domestic communications this is often referred to as data localization. Treated more broadly, to include the capability of a state to independently negotiate mutually beneficial arrangements with other states for ensuring safe passage of trans-border data flows,

exercising network sovereignty[46] becomes a more appropriate way to characterize this strategy. Many nations, including both China and the U.S., have indicated their respect for network sovereignty as a vital internet governance principle.[47]

Though a new term, network sovereignty is far from a new concept. It draws directly from the longstanding recognition that nation states have the right and duty to exercise superordinate control within their borders over all matters pertaining to the public good and to negotiate with other states on the basis of equality. Any such controlling entity exercises a form of network sovereignty when it constructs network systems ranging from transportation (e.g. roads, railroads, highways), utilities (e.g. water, electric) to communication (e.g. mail routes, telecommunication) in the public interest. As sovereign states, they can decide where these networks go, who or what can travel on them, at what price, what other networks to connect to or not and what basis, and so on.

Canadian national governments have pursued network sovereignty to serve national purposes in a variety of contexts since Canada's founding in the late 19th century. Indeed, its history as an independent nation can be read as the strategic development of transportation and communication networks designed to foster closer economic, cultural and political connections across its vast territory while warding off encroachment from the U.S. The most prominent example is the federal government's underwriting, in the 1880s, of the construction of the 4,000+ km transcontinental railway from Montreal to Vancouver. This remarkable undertaking is now popularly known as "The National Dream," and widely considered a central feature of Canada's founding mythology.[48]

Network sovereignty has also been a focus of Canadian media and telecommunications policy since the early 20th century. In the 1920s, in response to U.S. based radio stations broadcasting their signals well beyond the U.S. border and into Canadian population centres, radio entrepreneur Graham Spry led a successful movement to establish a nation-wide public broadcasting system, based on the premise that the airwaves were public property to be used in the public interest. Spry remarked famously, "It is a choice between the State and the United States."[49] Indeed, the concern that the U.S. could "cover" Canada in a grid of surveillance suggests that perhaps Spry's words are just as relevant now as they were almost 100 years ago.

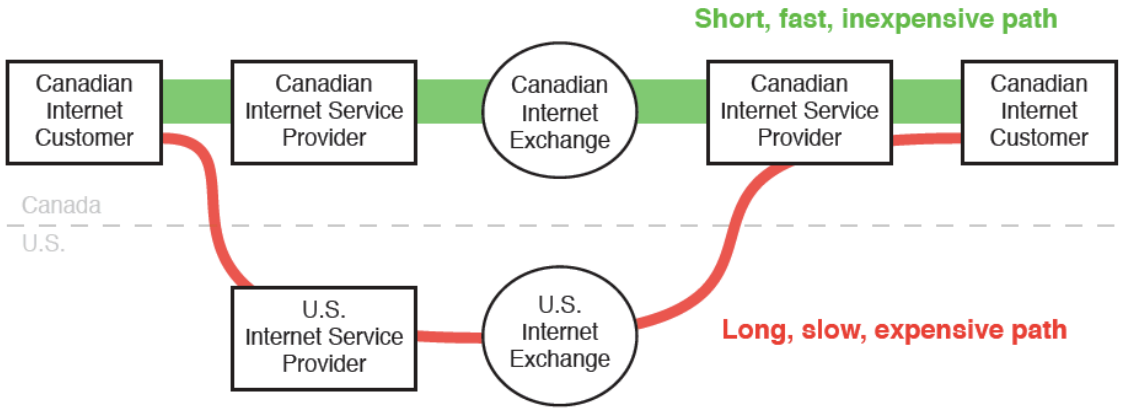
In keeping with the long history of protectionist communication policy, the Canadian Telecommunications Act of 1993, still in effect to this day, effectively mandates Canadian internet network sovereignty. The connection between the national telecommunications system, national sovereignty and individual privacy is clear. The Act states that "telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty." Among the various objectives of Canadian telecommunication policy, 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." Furthermore, a primary objective for this system is "to contribute to the protection of the privacy of persons."[50]

Canadian governmental adoption of network sovereignty in the internet realm has so far been mainly limited to building up internal network capacity and accessibility. In terms of data localization, only the federal government and two provinces, British Columbia and Nova Scotia, require that governments store Canadians' personal data within Canadian territory. Currently there are no similar requirements in the case of the internet routing of personal data. Adopting as official public policy the internal routing of domestic internet

communications promises to be a positive step in protecting Canadians' human rights. It would also be very much in keeping with Canada's historical development as an independent democratic nation.

Ensuring national routing for domestic communications doesn't just help to keep personal data away from the NSA and under the legislative and constitutional rights protections of national jurisdiction: it can also provide other significant benefits, notably reduced latency, economic efficiency and greater cyber-security. These are important goals for those seeking 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,"[51] is concerned that dependence on U.S. 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 US and found significant inefficiencies with the latter. (See Figure 8.)

Figure 8: Boomerang routing from an efficiency perspective[52]



In response, CIRA has actively pursued a strategy of data localization focused on internet routing, in recognition of the valuable role that internet exchange points (IXPs) can play in promoting efficient routing and keeping data within local regions. Noting that Canada is far behind other countries in developing IXPs, and specifically that in 2012 the US had 85 whereas Canada had just 2, CIRA has actively promoted the development of more IXPs across Canada. CIRA identifies the key benefits of this approach as 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.[53]

Since 2012 CIRA has assisted in opening three additional public IXPs, with more on the way. Studies have not yet been conducted to determine whether this contributes to keeping

Canadian domestic traffic within Canada, but it is interesting to observe that in this context promoting human rights aligns well with national economic interests.

Network sovereignty as international connectivity

Pursuing a strategy of internet traffic localization has its critics. The most prominent argument is that it promotes 'Balkanization,'[54] the fragmentation of the internet along national, geographic, commercial, religious or other lines accompanied by the erection of borders that inhibit the free flow of communication across them. Characterized as a 'splinternet',[55] this is presented as a betrayal of the ideals of a global, open internet free of externally imposed restrictions. Such barriers can be observed emerging in many countries in the form of censorship and filtering, but at the physical layer, building national infrastructure to keep domestic traffic local is not inherently balkanizing in the negative sense indicated above. If also combined with installing fibreoptic cables that more directly connect countries to each other, while avoiding U.S. transit, this exercise of network sovereignty can help to strengthen the internet globally. Increasing redundancy by creating alternative internet paths promotes resiliency, so there will be routing options in the case of interference or other forms of blockage when transiting intermediary states. The best publicized example of this is former Brazilian President Dilma Rousseff's proposal to construct a submarine fibreoptic cable from Brazil to Europe, explicitly to bypass the U.S. and NSA surveillance. Speaking at a joint news conference with the presidents of the European Commission and the European Council, Rousseff reaffirmed core internet values stating:

> We have to respect privacy, human rights and the sovereignty of nations. We don't want businesses to be spied upon … The Internet is one of the best things man has ever invented. So we agreed for the need to guarantee ... the neutrality of the network, a democratic area where we can protect freedom of expression. [56]

Viewed in light of Figure 2: 'U.S. as World's Telecommunications Backbone,' the trans-Atlantic Eulalink project, with a planned capacity of 30Tbps,[57] will dramatically increase internet connectivity between Europe and South America, advancing communications security and improving internet resiliency. As noted earlier, Canada is in a similar position as Brazil in terms of dependence on the U.S. for communication across both the Pacific and Atlantic Oceans. It has not yet so far developed similar public network sovereignty ambitions.

It is important to note that while the focus here has been on privacy risks of routing via the U.S. and hence NSA interception, this is not to suggest that keeping Canadian domestic internet traffic within Canadian borders or avoiding U.S. transit when communicating with third countries would fully shield Canadians from mass state surveillance. It is now well-documented that Canada's own signals intelligence agency, the Communication Security Establishment (CSE), is involved in a variety of domestic surveillance activities, including the potential capture of internet communication metadata of millions of Canadians.[58] This domestic surveillance raises the same serious privacy and other human rights concerns as those addressed above. Addressing these concerns by reforming Canadian laws as well as bringing security and law enforcement agencies demonstrably within legal and constitutional bounds is urgent and challenging. A spectrum of Canadian privacy and civil liberties organizations are working actively toward these goals. But however difficult it may be to achieve them, they are much more within the collective grasp of the citizenry than is the task of remedying U.S. government activities. Exercising Canadian network sovereignty

in terms of routing, so that data avoids U.S. transit, promises higher legal protection than if data is also exposed to NSA interception.

In sum, network sovereignty and reforming state surveillance at home is consistent with an internet governance regime that respects international human rights laws, and would contribute to protecting the privacy of internet users everywhere from state surveillance, foreign and domestic.[59] Asserting network sovereignty at a technical infrastructural level offers a powerful, even necessary means for promoting human rights on the internet. Even in combination with robust encryption, however, these approaches alone are not sufficient for accomplishing this goal. Ultimately, as in governing every other vital global resource such as the high seas, atmosphere, and electromagnetic spectrum, international internet governance requires effective binding rules that enjoy the support of all parties. The internet has reached a similar status as a global commons upon which many facets of contemporary life and our shared future depend. Since the Internet is a widely used communicative, expressive medium, the Universal Declaration of Human Rights and its accompanying International Covenant on Civil and Political Rights apply directly to it. As is inherent with such international treaties, especially given the transborder character of the internet, national sovereignty is willingly constrained for mutual benefit. Those promoting privacy on-line, whether through exercising network sovereignty or robust encryption, need also to help advance a global internet governance regime that respects these international legal norms. The *Necessary and Proportionate Principles* offer invaluable assistance in this important effort.

Conclusion

Thanks to Snowden's revelations, we now know that the signals intelligence agencies of the Five Eyes countries have covertly constructed a global internet surveillance apparatus capable of intercepting nearly all internet traffic. While we know much less about the internet surveillance that other countries are conducting, we know that it too is occurring, if perhaps not at the same scale. Such secret, unregulated mass surveillance presents fundamental threats to forms of internet governance that seek to ensure that the global communication infrastructure operates for the public good. In particular, mass surveillance violates the protection of privacy, freedom of expression and other human rights enshrined in international law. The 13 *Necessary and Proportionate Principles*, based on well established and widely endorsed legal rights, provide a valuable framework for bringing state surveillance legislation and practices within internationally accepted norms. Within such a framework, the principle of Transparency, applied to internet operations and actors, is a necessary feature of internet governance as well as a potentially fruitful focus for related research. In particular, transparency tools for probing obscure but policy relevant aspects of internet infrastructures, such as the IXmaps mapping platform, can be effective aids for internet governance research. Used in the context of Canadian internet routing, as one example, this mapping tool indicates that a significant portion of domestic traffic travels via the US where it is exposed to NSA surveillance. In addition, analysis of routings between Canada and third countries suggests that a far greater proportion of internet traffic also transits the US. This supports an argument that network sovereignty – understood as a country ensuring that its internal communications can be kept within the national territory and legal jurisdiction, as well as that it is able to keep its international communications relatively independent of intermediary states that can secretly and unilaterally intercept or interfere with this communication – has a fruitful role to play in developing a robust international internet governance system that serves the global public interest.

Acknowledgements

The IXmaps project is the work of an extensive research team that began its work in 2009. Currently active members are Colin McCann, Antonio Gamba, Jonathan Obar and Dawn Walker. The project has been supported by the Social Sciences and Humanities Research Council of Canada (SSHRC), the Office of the Privacy Commissioner of Canada (OPC) and the Canadian Internet Registration Authority (CIRA). We are also grateful to those individuals, largely anonymous, who collectively have contributed over 100,000 traceroutes to the database by installing and running our customized traceroute generation program. See: http://IXmaps.ca/contribute.php

The Snowden Surveillance Archive, a fully searchable, complete collection of published Snowden documents, was helpful in conducting this research. George Raine, Jillian Harkness and Evan Light developed the Archive with funding from the Social Sciences and Humanities Research Council of Canada (SSHRC) and Fonds de recherche du Québec – Société et culture (FRQSC). The Canadian Journalists for Free Expression (CJFE) hosts the Archive at https://snowdenarchive.cjfe.org.

Author's biography

Andrew Clement is a Professor Emeritus in the Faculty of Information at the University of Toronto, where he coordinates the Information Policy Research Program and co-founded the Identity Privacy and Security Institute (IPSI). With a PhD in Computer Science, he has had longstanding research and teaching interests in the social implications of information/communication technologies and participatory design. Among his recent privacy/surveillance research projects are: the Snowden Surveillance Archives, an on-line searchable collection of all documents leaked by former NSA contractor Edward Snowden subsequently published by news media; Seeing Through the Cloud, which examined extra-national outsourcing of eCommunications services, especially by universities; IXmaps.ca, an internet mapping tool that helps make more visible NSA mass internet surveillance activities and the routing of Canadian personal data through the U.S. even when the origin and destination are both in Canada; SurveillanceRights.ca, which documents (non)compliance of video surveillance installations with privacy regulations and helps citizens understand their related privacy rights; and Proportionate ID, which demonstrates through overlays for conventional ID cards and a smartphone app privacy protective alternatives to prevailing full disclosure norms. Clement was a co-investigator in the seven year major research collaboration, The New Transparency: Surveillance and Social Sorting and a collaborator in its successor project, Big Data Surveillance.

Endnotes

[1] See Author's bio.

[2] *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, May 2014, p. 2. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

[3] The portions of this paper dealing with the NSA surveillance programs and the IXmaps internet mapping tool have been adapted from several prior research publications:
Andrew Clement & Jonathan Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges," Chapter 1 in Michael Geist (ed), *Law, Privacy and Surveillance in Canada in the Post- Snowden Era*, University of Ottawa Press, 2015, pp 13-44. Available for free, open access download at http://www.press.uottawa.ca/law-privacy-and-surveillance or http://hdl.handle.net/10393/32424
Andrew Clement, "NSA Surveillance: Exploring the geographies of internet interception", *Proceedings of the iConference* 2014, Berlin, March 4-7. Preprint available at: https://www.dropbox.com/s/35s52dxv87zb6jo/iConf14%20paper%20-%20NSA%20Surveillance%20and%20Geographies%20of%20internet%20interception%20Oct%2017.pdf
Andrew Clement, "IXmaps – Tracking your personal data through the NSA's warrantless wiretapping sites", *Proceedings of the 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

[4] James Bamford:
The Puzzle Palace: A Report on N.S.A., America's Most Secret Agency, 1982
Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. 2002
The Shadow Factory: The UltraSecret NSA from 9/11 to the Eavesdropping on America, New Y ork: Doubleday, 2008.
"The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". *Wired.* March 15, 2012.
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[5] James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times,* December 16, 2005. http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

[6] Glenn Greenwald: *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* Hamish Hamilton, 2014, p. 90.

[7] Floor Boon, Steven Derix and Huib Modderkolk "NSA infected 50,000 computer networks with malicious software", *nrc.nl,* 23 November 2013 http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487
Note that this image does not show the domestic interception within the Five Eye countries. It also indicates that the NSA had "infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information."

[8] These and the following figures showing secret NSA documents come from the collection that Snowden turned over to journalists. The sources cited indicate the first publication. They can also be found in the Snowden Surveillance Archive, a complete collection of all documents that former NSA contractor Edward Snowden disclosed in June 2013 to journalists Laura Poitras, Glenn Greenwald and Ewen MacAskill, and published between then and September 2016: https://snowdenarchive.cjfe.org

[9] Source: *Washington Post*, NSA slides explain the PRISM data-collection program, June 6, 2013, Updated July 10, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[10] Barton Gellman and Laura Poitras, U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, *Washington Post*, June 6, 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

[11] Barton Gellman and Todd Lindeman, Inner workings of a top-secret spy program, *Washington Post,* June 29, 2013 http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/

[12] Ryan Gallagher & Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware" *The Intercept*, March 12 2014 https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

[13] The nuclear submarine, Jimmy Carter, has been specially modified to conduct these under water cable tapping operations. See: Associated Press, New Nuclear Sub Is Said to Have Special Eavesdropping Ability, *New York Times*, February 20, 2005. http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0

[14] James Ball, NSA's Prism surveillance program: how it works and what it can do, Guardian, 8 June 2013 http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

[15] Glenn Greenwald, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', Guardian, 31 July 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[16] *Guardian,* Boundless Informant: NSA explainer – full document text, June 8, 2013 http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text

[17] *Guardian*, Boundless Informant NSA data-mining tool – four key slides, June 8, 2013. http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides

[18] Glenn Greenwald and Ewen MacAskill, Boundless Informant: the NSA's secret tool to track global surveillance data, *Guardian*, 11 June 2013. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

[19] Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *Guardian,* 31 July 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[20] Sean Gallagher, Building a panopticon: The evolution of the NSA's XKeyscore, *ArsTechnica*, Aug 9 2013. The need for these globally distributed caches may well be temporary, given the massive Utah data centre that Bamford reported on in 2012 and is now operational.

[21] *Der Spiegel.* "'Prolific Partner': German Intelligence Used NSA Spy Program", July 20, 2013.

[22] Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *Guardian,* 31 July 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[23] Reporters Without Borders, *Enemies of the Internet 2014: entities at the heart of censorship and surveillance,* 12 March 2014 http://12mars.rsf.org/2014-en/#slide2

[24] ICANN, *Who Runs the Internet?*, https://www.icann.org/news/multimedia/78

[25] *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*, May 2014, p. 2. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

[26] *Universal Declaration of Human Rights*, Article 12. http://www.un.org/en/universal-declaration-human-rights/, which reads:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[27] *International Covenant on Civil and Political Rights*, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

[28] *Necessary and Proportionate,* op cit, p. 3

[29] *Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance,* May 2014, p. 31. http://necessaryandproportionate.org/LegalAnalysis

[30] *Necessary and Proportionate,* op cit, p. 10

[31] https://en.wikipedia.org/wiki/Informational_self-determination

[32] See respectively:) http://www.caida.org , http://www.measurementlab.net/ https://atlas.ripe.net/ https://www.pch.net/ https://planet-lab.org/

[33] The IXmaps name derives from internet exchange mapping. The original idea for this came from Nancy Paterson, an artist/academic at OCAD University. Together with David Phillips, a colleague in the Faculty of Information, University of Toronto, we successfully sought funding from the Social Sciences and Humanities Research Council of Canada (SSHRC) to develop the traceroute generation and mapping software that remains at the core of the current platform. See http://IXmaps.ca

[34] Determining the geographic location of a router based on its IP address is a widespread practice in the internet industry. However, achieving reliable geo-location is notoriously difficult, especially in the case of core routers that appear at intermediary hops of traceroutes. We base an initial approximation of location on the publically available information from the popular Maxmind Geolite free geolocation service. <http://dev.maxmind.com/geoip/legacy/geolite/ > As Maxmind notes, "IP geolocation is inherently imprecise." To improve accuracy we selectively correct router locations based mainly on automated hostname parsing scripts we have developed, as well as manual route topology and latency analysis. To help identify and correct the location of misplaced routers, we invite IXmaps users to flag suspect routers and suggest improved locations.

[35] Another internet policy issues that the IXmaps platform has been be used to investigate is the transparency of ISPs in terms of their privacy policies. See: https://www.ixmaps.ca/transparency.php We are also researching the location of suspected Five Eyes surveillance sites globally to enable determining which traffic external to the U.S. is also susceptible. So far we have added information on the location of NSA partner telecom carriers AT&T and Verizon facilities worldwide to the database. See the AT&T/Fairview and Verizon/Stormbrew layers on the IXmaps Explore page: https://www.ixmaps.ca/explore.php

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

[37] PBS Frontline. *Spying on the Home Front*, May 15, 2007.

[38] This percentage should be treated as a rough estimate of actual internet traffic. Biases in the sample of traceroutes contributed by users to the database, as well as endemic difficulties in accurately geo-locating routers based on hostnames, IP addresses and latencies, mean that the relative amount of domestic U.S. traffic that could by intercepted by NSA splitters installed in these 18 cities needs to be treated with caution. Traceroutes do not reflect actual volumes of traffic. 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 Clement, A. "IXmaps – Tracking your personal data through the NSA's warrantless wiretapping sites" IEEE - ISTAS conference, Toronto, June 26-27, 2013.

[39] Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras and James Risen, AT&T Helped U.S. Spy on Internet on a Vast Scale, *New York Times,* Aug. 15, 2015

http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=1

[40] William B. Norton, *The Internet Peering Playbook: Connecting to the Core of the Internet,* DrPeering Press, 2012, p. 71.

[41] http://submarine-cable-map-2014.telegeography.com/

[42] Data collected by IXmaps supports this pattern, in that there are currently 10 times as many international traceroutes destined for a third country that are routed through the US (130) as do not show US routing. However, these figures need to be treated with caution since we have so far made no systematic attempts to collect, geo-locate and analyse 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 U.S. based gateways, or more clandestinely via submarine or landing point interception.

[43] As noted above, these results need to be treated with caution, especially since they are based on a relatively small and hardly representative sample of routes. Notwithstanding these important limitations, this significant proportion of routes transiting the U.S. is consistent with what is known about global internet infrastructure from other sources and reinforces the importance of third country routing as an internet governance policy issue. It also suggests a fruitful direction for further research.

[44] *Necessary and Proportionate,* op cit, pp xii, 36-38.

[45] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A.HRC/23/40, 17 April 2013), para. 79.

[46] Internet sovereignty and cyber-sovereignty are synonyms in this context.

[47] Sun Mengxi, "Network sovereignty extends int'l framework to Internet," *Chinese Social Sciences Today,* June 23, 2016. See: http://www.csstoday.com/Item/3563.aspx

[48] Pierre Berton, *The National Dream*, McClelland and Stewart, 1970

[49] Marc Raboy, *Missed opportunities: The story of Canada's broadcasting policy.* Montreal, QC: McGill--Queen's University Press. 1990. p. 40

[50] Telecommunications Act, 1993, Section 7 http://laws-lois.justice.gc.ca/eng/acts/T-3.4/page-2.html#h-6

[51] Canadian Internet Registration Authority (CIRA). "The CIRA vision and mission." https://cira.ca/about-cira

[52] Woodcock, Bill & Edelman, Benjamin, Toward Efficiencies in Canadian Internet Traffic Exchange, Canadian Internet Registration Authority, Sept 2012, http://www.cira.ca/assets/Uploads/Toward-Efficiencies-in-Canadian-Internet-Traffic-Exchange2.pdf

[53] Ibid, p. 1

[54] Sascha Meinrath, "We Can't Let the Internet Become Balkanized, The backlash to U.S. surveillance threatens the foundation of a free and open Web," *Slate*, Oct. 14 2013 http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html

[55] https://en.wikipedia.org/wiki/Splinternet

[56] *Reuters,* Brazil, Europe plan undersea cable to skirt U.S. spying, Feb 24, 2014 http://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224

[57] *Reuters,* Telebras faz acordo com IslaLink para cabo submarino América do Sul-Europa, June 30, 2015 http://br.reuters.com/article/internetNews/idBRKCN0PA2KM20150630

[58] Bill Robinson, "CSE: What do we know? What do we need to know?" Lux Ex Umbra blog post, October 09, 2016 http://luxexumbra.blogspot.ca/2016_10_01_archive.html

[59] Andrew Clement & Jonathan Obar, *op cit*