PART II

LEGAL ISSUES

Page left blank intentionally

CHAPTER III

Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation

Tamir Israel

The recent and dramatic expansion of foreign intelligence surveillance activities, revealed definitively in a trove of documents made public by former NSA analyst Edward Snowden, can be traced to a few drivers. First and foremost, technical changes have made an immense amount of data practically accessible and analyzable in ways that have no precedent in human history. Most of our activities have migrated to digital networks, raising distinct implications in the foreign intelligence-gathering context. Digital networks do not route in direct lines.[1] Moreover, most digital interactions are intermediated through one or more entities, often based in foreign jurisdictions. Cloud-based data is often stored redundantly on multiple servers, each in its own jurisdiction. Foreign intelligence agencies can now clandestinely monitor the world's communications from their own territory, without the practical impediments inherent in sending agents to foreign lands. Additional technical interoperability between foreign intelligence partners, particularly within the Five Eyes partnership (Australia, Canada, New Zealand, the United Kingdom, and the United States) (hereafter FVEY) has facilitated an unprecedented integration of foreign intelligence capacities, extending the monitoring and analysis capacities.[2] Finally, technical advances in data *storage* make retention of vast amounts of information possible in ever-growing volumes.[3]

At the same time, foreign intelligence has been rapidly shifting its focal point from foreign states and their agents (the Cold War "spy

vs. spy" paradigm that characterized much of the history of Western foreign intelligence agencies) to a "spy on everyone" mindset driven by a terrorist-based threat matrix and a new collect-it-all mentality.[4] This operational shift has had tangible impacts as agencies begin to push the limits of their already broad powers and their ever increasing technical capacities to collect, analyze, and keep "everything."

These shifts in technical capacities and intelligence culture have been accompanied by broadly framed legal powers that do little to check excesses that might result. Canada's foreign intelligence agency, the Communications Security Establishment (CSE), derives its legal mandate and surveillance authorization framework from Part V.1 of the *National Defense Act (NDA)*.[5] The framework is modelled on the same rationale and general structure as that of other FVEY agencies — open-ended powers limited primarily by an obligation to limit the exposure of domestic individuals and a need to show some nexus to a foreign intelligence objective.[6]

The analysis below argues that the core limitations placed on CSE in its foreign intelligence mandate are ineffective at constraining its activities.[7] Before embarking on this substantive assessment, however, we first describe shortcomings in CSE's control structure, which exacerbate the inherent breadth of its legal restrictions by focusing too heavily on oversight.

Oversight and Accountability: Loose Assurances of Legality from behind a Veil of Secrecy

CSE is subjected to minimal legal control, even when measured by the standard of its FVEY partners.[8] The NSA, for example, operates under similarly broad legal restrictions, but is subjected to some non-partisan legislative and loose judicial control.[9] CSE's legal restrictions can in essence be reduced to four primary constraints. It relies on ministerial authorizations (to intercept private communications) or ministerial directives as lawful authority for its privacy invasive activities. Its activities must be in pursuit of its mandate, statutorily defined in the NDA (the *Privacy Act* also limits it to collecting information relevant to its mandate).[10] It is statutorily prevented from directing its activities at Canadians. It cannot, of course, violate the *Charter*. The substantive scope of each is explored in more detail in the following sections. Here, we examine how the executive branch essentially interprets and applies these legal restraints on its own, with

no external controls from either the judiciary or legislative branch of government. The executive is effectively left as the primary if not sole arbiter of its own legal restraints. Against this backdrop, official defence of CSE often amounts to publicly compelling, yet ultimately meaningless, statements that CSE "operates within the law."

As in many contexts, the modern technological era poses great challenges, as legal concepts struggle to keep pace with rapidly evolving and highly complex contexts. This leads to many ambiguities that are central to the scope and nature of the legal restraints imposed on CSE. Determination of these ambiguities can significantly change the scope of permitted activities. While *Charter* privacy protections should develop in a technologically neutral manner,[11] understanding the implications of shifting practices in new technological mediums can be a difficult exercise, confounding attempts at oversight and control.[12] In the absence of rigorous and adversarial challenge, these ambiguities and complexities are often resolved in favour of the foreign intelligence agency that is implementing the powers in question.

Even in the presence of judicial control (but lacking adversarial input and with only a loose review mandate), understanding the evolving technical landscape has been difficult. The Foreign Intelligence Surveillance Court (FISC), for example, found in 2011 that the NSA Internet surveillance program it had been regularly approving for five years was significantly broader in scope than it had understood: "[The Government] disclosed… for the first time that NSA's upstream collection of Internet communications… may contain data that is wholly unrelated to the tasked selector."[13] The "Upstream" program referred to is one of the NSA's most expansive electronic surveillance mechanisms.[14] It, along with its sister program PRISM, harvests billions of transactions from communications networks daily, most of which are retained for thirty days, with hundreds of millions retained longer term.[15] Since 2006, FISC had believed it was approving interception of discrete communications of specific targets. In 2011, it realized entire Internet transactions were being collected, indiscriminately sweeping up mass amounts of domestic and untargeted data alongside each discrete target, yet the program had been regularly approved for five years without this central understanding. A process open to adversarial input would have forced FISC to confront this factual inaccuracy far sooner.[16]

Similar issues have arisen with respect to CSE's activities. The Federal Court found in *Re X* that it had significantly underestimated

the scope of activities undertaken by CSE when authorized to assist Canadian Security Intelligence Service (CSIS) monitor communications of Canadians abroad.[17] Since 2009, the court had understood it was authorizing the monitoring of such communications as they transited through Canadian-based networks.[18] However, CSE was secretly tasking its FVEY partners' formidable intercept capacities in conjunction with this "from home" surveillance.[19] The government's defence of its omission was that it required no authorization in this context. It is an interpretation that highly favours its position and robs the court of the ability to evolve the law to account for new realities, such as the increasingly expansive scope of FVEY surveillance capabilities. However, this legal interpretation is not patently unreasonable.[20] It should not be a surprise that the government, on its own initiative and in the absence of adversarial input, reached this conclusion, or that it will reach similar conclusions in the future.

These examples demonstrate that even with the presence of nominal judicial scrutiny, applying legal restraints to the activities of foreign intelligence agencies has proven a challenge. Far from robust mechanisms for rigorous adversarial challenge, CSE operates without the prospect of even sparse external control. Given the clandestine nature of CSE's intelligence-gathering mandate, some secrecy is required. However, this does not mean CSE can be relieved of all public accountability and the rule of law. The application, interpretation, and implementation of the four legal constraints referred to above occurs primarily on the basis of internal legal opinions from the Department of Justice. Neither this underlying legal reasoning nor the ministerial authorizations and directives and CSE activities that are based on this reasoning are made public. Additionally, CSE is free from any parliamentary control or even scrutiny.[21] Canadians are left to trust, but can never verify legality.

Its primary oversight mechanism is the CSE commissioner, an autonomous former judge with independent budget appropriation.[22] The commissioner assesses CSE's activities for compliance with the various legal restrictions placed on it. Having access to secret CSE activities, internal documents, and even privileged opinions, the commissioner can provide a critical independent voice in internal CSE and ministerial decision making. In addition, the commissioner's annual reports can provide an avenue to enhanced public debate around CSE activities. However, the commissioner's recommendations are not binding and are often ignored on issues of central

importance.[23] Further, the commissioner's annual reports are cryptic, rarely providing meaningful insight into specific CSE activities.[24] They typically focus more on describing the commissioner's own oversight activities, with specific issues addressed at a high level of generality. As the commissioner never publicizes the legal reasoning underpinning his oversight (receipt of privileged communications may even prevent this),[25] there is no opportunity for the academic or legal community to challenge these without significant guesswork or a whistle-blower.

Problems with the existing framework abound. For example, CSE was granted the power to incidentally intercept private communications of Canadians under ministerial authority. Several commissioners disagreed with CSE's legal interpretation of this authority, arguing it unjustifiably broadened what CSE can do.[26] Successive commissioners were nonetheless obligated to assess the legality of CSE's activities based on its own prevailing interpretation. In his final report, Commissioner Lamer noted that his "one regret" was leaving his position "without a resolution of the legal interpretation issues that have bedevilled this office since December 2001."[27] CSE is often publicly defended with assertions that no commissioner had ever found CSE activities to be in violation of the law.[28] The value of these assessments is significantly undermined as they are premised on legal interpretations that the commissioners themselves found inadequate. It is concerning that meaningful details regarding the nature of the disagreements in question only emerged in the public reports in 2008—six years after they were first identified.[29] Even then, the object of the dispute was disclosed, but not the substance or legal basis of the disagreement.

Another example arises from *Re X*. In late 2013, Commissioner Décary's first post-Snowden annual report mentioned that CSIS had provided incomplete information to the Federal Court when it sought a new legal framework for CSE assistance in monitoring Canadians abroad in 2009.[30] The missing information in question led to a judicial reformulation of the legal framework for CSE/CSIS assistance.[31] Some have pointed to this as an example of a *functioning* CSE oversight system. However, CSE/CSIS did not comply with Commissioner Décary's recommendation to provide the court with more information. Mr. Justice Mosley, who had issued the initial 2009 framework authorization, read the report on his own volition and mandated CSIS/CSE to provide the information.[32] Justice

Mosley had no obligation to read this report and, had it not come to his personal attention, the reconsideration is not likely to have occurred. Moreover, this particular scenario implicated CSE in its (c) assistive mandate (see also note 7). CSIS must obtain prior judicial authorization to seek CSE assistance in intercepting private communications. Had a comparable scenario arisen with respect to CSE's independent foreign intelligence activities, there would be no Federal Court judge with jurisdiction to proactively assess the issue in this manner. In addition, important details that Justice Mosley found necessary for his assessment came from the Security Intelligence Review Committee's (tasked with reviewing CSIS) annual report, which provides significantly more substantive operational details.[33]

The Privacy Commissioner of Canada also has oversight powers with respect to CSE operations. However it, too, can only issue recommendations and only with respect to limited protections encoded in the *Privacy Act*. Both the Privacy and CSE commissioners provide valuable input into CSE's internal assessment processes, enhancing its attempts to properly account for important counter-interests such as fundamental rights and freedoms. Many of the recommendations that these bodies provide CSE are adopted voluntarily. However, a system that relies almost solely on secret internal policies and non-binding recommendations is not one constrained by law. Key disagreements over central legal ambiguities remain unresolved and colour all the assessments carried out by these bodies. In effect, the oversight occurs against a yardstick defined by CSE itself, "put[ting] at risk the integrity of the review process."[34] Such a system is not capable of ensuring that the extraordinary powers granted to CSE are being employed in a proportionate manner.

Ministerial Authorizations and Directives: Lack of Any Meaningful Control

Compounding the general secrecy that pervades CSE's accountability regime is a general lack of external control. The Minister of National Defence ("Minister") is the only entity empowered to legally control CSE, which relies on ministerial authorizations and directives as lawful authority for its surveillance activities.[35] The Minister is also able to issue further discretionary operational directives that are binding on CSE.[36] Neither Parliament nor the courts nor any independent tribunal play any role in controlling CSE. Like any government

action, CSE's activities can, of course, be challenged in court, as can its underlying statutory framework.[37] However, such challenges will by necessity be rare, as CSE's activities and the ministerial authorizations and directives that underpin them remain shrouded in secrecy. Also, CSE activities rarely appear in judicial proceedings. In the absence of a whistle-blower, adversarial legal challenge to CSE's expansive *activities* is unlikely.

Section 8 of the *Charter* requires that the state obtain prior authorization issued by an "entirely neutral and impartial" arbiter.[38] The purpose of section 8 is "to protect individuals from unjustified state intrusions upon their privacy," and this requires that a neutral arbiter determine whether a particular intrusion is justified, whenever possible. The minister is, in the words of one expert commentator, "many things, but a disinterested judicial officer he is not."[39] CSE receives its foreign intelligence target priorities from the minister (and the rest of cabinet). Specifically, the minister is responsible for establishing CSE's foreign intelligence-gathering priorities.[40] That the minister is at once the arbiter of investigative priorities *and* the legitimacy of investigative techniques used to achieve those priorities is deeply problematic. The minister of national defence would naturally be guided by a range of public policy and expediency concerns when setting CSE's intelligence priorities, rendering him incapable of acting judicially when determining whether a particular privacy invasive activity is or is not justified.[41]

Prior judicial authorization is the default requirement for constitutional privacy invasion, but the particular circumstances of a given context can justify departures from this general rule.[42] Diminished expectations of privacy, exigent situations, and investigative contexts where secrecy is necessary can all justify modifications from the standard procedural requirements.[43] However, in each of these instances, there must be some mechanism for meaningful judicial review and adversarial challenge.[44] Similarly, some (but not all) of CSE's intelligence-gathering activities relate to national security. However, the heightened concerns inherent in national security may not, in the absence of demonstrable practical challenges, justify forgoing judicial authorization with respect to digital interactions that attract high expectations of privacy.[45] In this context, the information obtained by these privacy invasive activities may result in adverse consequences for individuals (such as placement on a no-fly list or worse), but affected individuals are not likely to ever discover CSE

intelligence as the source of such impacts. The surveillance itself is highly surreptitious despite its far-reaching scope. Judicial review is a highly unlikely prospect.

Nor do the circumstances in question justify excluding the judiciary from the process. Ministerial authorizations were chosen in lieu of judicial authorization because it was presumed that Canadian courts lack the jurisdiction to authorize surveillance activities occurring in foreign territories.[46] This is no longer a sustainable premise. Indeed, Bill C-44, which became law on April 23, 2015, explicitly grants Canadian judges the ability to "authorize activities outside Canada to enable [CSIS] to investigate a threat to the security of Canada."[47] CSE is permitted to assist CSIS in carrying out these extraterritorial investigations.[48] A similar provision could readily be employed to ground judicial authorization of CSE surveillance activities abroad. CSIS is tasked with a similar investigative mandate and operates under prior judicial authorization.[49] There is no practical reason not to impose some form of judicial control onto CSE.

The provisions guiding CSE's authorization are equally problematic, and so broad that even a court would have difficulty constraining CSE's activities through them. The minister may authorize CSE to "intercept private communications in relation to an activity or class of activities" if satisfied that Canadian privacy is protected, that the information could not be otherwise obtained, and that the anticipated value of the intelligence justifies the interception.[50] Because authorization occurs on the basis of "activities or classes of activities," consideration of whether the "particular interests that could be compromised" by the authorized surveillance justify it or not occurs at a high level of generality and fails to account for specific privacy interests.[51] The lack of a clear reasonable grounds standard to measure the authorization justification framework exacerbates this breadth.[52] Courts have recognized that national security investigations may require a different kind of specificity than traditional criminal investigations, tailored to the anticipatory nature of the investigations.[53] However, Canadian courts have *not* accepted the proposition that national security concerns can justify a lower standard for invading high expectations of privacy.[54] The breadth of the current standard allows CSE almost limitless latitude in determining the scope of its privacy-violating activities.

As broad as the legislated authorization standard is, CSE has interpreted it to be even broader — the Minister need only authorize

"classes of communications interception activities," as opposed to interceptions of private communications in relation to specific activities or targets. Commissioners have noted that this interpretation is not supported by the statute and unduly expands CSE's authorization regime.[55] It allows the Minister of National Defence to frame his authorizations so broadly that only three are required for CSE's entire foreign intelligence interception program.[56] This alone speaks to their expansive breadth and lack of specificity.

Commissioners have also pointed to CSE's misinterpretation of the term "interception" as having obscure "legal and operational significance."[57] We know that most FVEY interception programs rely on network level filtering — all network traffic and phone calls are continually searched for matches on tasked keywords.[58] CSE itself has over two hundred sensors filtering network traffic around the world, and is further able to task other FVEY agency interception resources.[59] Some FVEY agencies only consider an interception to occur when network traffic is "accessed." Filtering conducted by ISP equipment (under order from the agency) is not engaged.[60] Another argument sometimes presented by FVEY agencies is that "interception" only occurs (and privacy is only implicated) when specific communications are acquired and retained. For example, the commissioner recently described CSE's wiretapping activities only in terms of "accidentally collected" and "retained" private communications, while ignoring how many private communications were "searched" for keywords.[61] Either argument greatly skews the privacy analysis by disregarding significant analytical activity — the private communications of millions can be scoured for selectors, yet only the "hits" count. Non-collected communications monitored for keywords are clearly "searched," if only to confirm that they do *not* include the keyword in question.[62] Simply knowing that one's communications are being scanned for certain words can have a serious chilling effect.

CSE's legal framework is also flawed in its application to "metadata," data *about* a communication. CSE is operating under the assumption that metadata is not considered a "private communication."[63] As a result, CSE's activities (its own collection as well its use of FVEY resources) are different in character and scope if it classifies data as "metadata" or "content." Metadata does not fall under the ministerial authorization regime, which only regulates interception of private communications. Instead, under a single ministerial directive, CSE gathers "huge amounts" of metadata, "on large numbers

of people."[64] Internet metadata is often difficult to distinguish from "content": a Facebook ID provides you with access to the profile itself; a URL permits you to see the web page or other resource viewed; the URL for an online search will include the search query.[65] Even traditional phone metadata can be highly revealing of the objects of the call itself.[66] Whereas most definitions of metadata exclude data that would reveal the purpose of the communication it relates to, CSE defines it broadly.[67] It includes URLs of web resources, Facebook identifiers, search queries, and even document-authoring information.[68] There is no basis for treating such metadata differently from content; they equally implicate our private lives.[69]

Attempts to moderate the inherent breadth of CSE's lawful authorization come in the form of targeting and minimization limitations. These involve general processes (explored below) designed to limit impact on Canadian privacy, not to target surveillance on intelligence targets.[70] Even if effective, such mechanisms would never be reassuring, as CSE would still be able to monitor all communications indiscriminately and will have infiltrated the infrastructure necessary to do so. Its powers are so broad that they disregard the privacy of millions around the world in order to obtain small iotas of potentially useful information. For example, one Government Communications Headquarters, or GCHQ, input into a joint FVEY resource collected millions of Yahoo customer private video chats, without regard to whether specific accounts were targets or not.[71] GCHQ explored expanding this intake to include video/audio cameras increasingly found in living rooms.[72] One sample of NSA-acquired and retained communications data revealed medical records, resumes, children's academic transcripts, sensitive pictures, and embarrassing comments of innocent individuals.[73] The ratio of targeted to non-targeted individuals whose data was collected and retained in this sample was 1:9 (not counting irrelevant information on targets). Once collected, mining of this dataset is determined by CSE itself, not the minister, and not on the basis of any individualized suspicion of wrongdoing. While the *Privacy Act* imposes a "relevance" requirement, other agencies have defined this to mean a "two-to-three degree of separation" model of suspicion, which scales rapidly on digital networks.[74] Moreover, while the NSA relevance criteria are at least tied to a particular investigation, CSE's relevance is only tied to its general foreign intelligence mandate.

Even as the sensitivity of digital data has increased over the past decade, FVEY agencies have decided that "all" communications are relevant to their mandate because they generate general intelligence capacities that are useful.[75] Doubtless, these various programs have had some investigative value in important efforts to prevent serious threats to life and limb. But their formulation makes no attempt to account for the disproportionate impact this approach has on our private digital lives. The prevailing "collect everything" mindset is not effectively mitigated by minimal steps to limit subsequent access and use. As explored in the next section, the near-limitless mandate that governs the use of these collected treasure troves is, on the one hand, far broader than the existential terrorist threat that is often its public face and, on the other, poses a direct threat to democracy as we know it.

Foreign Intelligence: A Mandate with Few Limits and Substantial Potential for Abuse

Defences of the incredibly broad powers granted to CSEC and its Five Eyes counterparts often focus on the need to prevent serious terrorist or other existential threats; however, this is a "misleadingly narrow sales pitch."[76] The term *foreign intelligence* itself is defined in broad terms as information "about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security."[77] It couples a strong focus on counterterrorism with an enduring interest in political intentions and a general need for situational awareness.[78] Substantively, this has evolved to include a broad range of objectives and intelligence agencies have used their powers to further political or economic objectives and, fundamentally, as a vehicle for advancing *any* national interest.[79] The mandate is problematic for its all-inclusiveness, but also for its application to the intentions of foreign individuals who are neither representatives of a foreign power nor agents of a terrorist organization. As the need to act within its mandate (and restrict collection to mandate-relevant intelligence) is one of the central substantive limitations on CSE's surveillance activities, this breadth of purpose and application is concerning.

Expansive foreign intelligence powers are increasingly used to gain domestic economic and political advantages. Information is gathered to "assist a [FVEY] member government engaged in

sensitive international negotiations — be they diplomatic or economic."[80] Foreign intelligence agencies are playing a bigger role in advising the government on economic decision making.[81] A recent government focus on international trade agreements is expected to lead to even greater government "demands for information on… economic/prosperity issues."[82] It can also include situational awareness of various economic and political issues that Canadian cabinet ministers decide are priorities.[83] This has included, for example, use of extensive FVEY surveillance capacities to spy on the Brazilian ministry in charge of mining rights, to spy on economic meetings such as the G20 summits in London and Toronto, to seize data from the lawyer of a foreign government in the midst of negotiations, to insert malicious spyware targeting trade institutions within the EU, to directly exploit private networks used by businesses such as banks and telecommunications companies, and to spy on other countries in preparation for a summit on environmental issues.[84] It has even included targeting of UN Secretary General Ban Ki-Moon for the less than life-preserving objective of obtaining his talking points in advance of a meeting with President Obama.[85] These objectives accompany the more serious national security concerns, and the same investigative techniques (the same databases, in fact) fuel both. Moreover, FVEY mandates also include "understanding the global communications infrastructure," a broad and open-ended objective that appears to permit random and unfettered experiments on collected data.[86]

With respect to terrorism, it has long been recognized that an unchecked security investigative mandate poses a serious threat to core democratic values. This threat arises from the open-ended nature of security investigations and the close proximity between security concerns and unpopular (but important) political views, making privacy protections all the more important in this context.[87] The inherent breadth of the security concept, which necessarily adopts an open-ended threat model, renders attempts to prevent detrimental impact difficult.[88] Recent examples have confirmed that the temptation to use expansive security-based powers for other objectives is difficult to resist. Australia was recently rebuked for spying on communications between East Timor and its lawyer in the course of an arbitration dispute, putatively for national security.[89] Canada's own domestic experience with security intelligence confirms this — decades of abuse of security power harmed legitimate

political activities, forcing Parliament to sever security intelligence investigations from the RCMP's mandate and vest these in an independent agency, CSIS.[90] CSE itself is expressly empowered to assist domestic agencies with their own respective investigations, and repurposes its vast intelligence holdings when doing so.[91] Far from taking steps to address these problems, CSE's foreign intelligence mandate heightens the threat by overtly combining political and economic objectives alongside security.

Historically, the inherent breadth and heightened human rights risk inherent in the foreign intelligence concept were tempered by a focus on foreign powers and their agents.[92] In the wake of 9/11, this focus was broadened to include not only terrorist organizations and their agents but any information about the "intentions" of any "foreign individual" in relation to "international affairs." We have since seen the formidable powers of FVEY agencies levelled at individual financial transactions conducted through text messaging;[93] prominent Muslim community leaders with no terrorist affiliation;[94] civil society groups engaged in public advocacy on human rights issues;[95] and journalists critical of the US government's response to 9/11.[96] Some FVEY agencies have carried out cyber attacks designed to disrupt online discussion forums used by hacktivists and political dissidents.[97]

This is problematic because the integrated nature of modern digital networks not only places most individual interactions within reach of FVEY surveillance systems, but also leads to policy resolution that increasingly occurs on the international stage. Much of this now falls within the potential purview of foreign intelligence agencies, as it relates to the "intentions" of "foreign individuals" in relation to "international affairs." As argued in the next sections, this integration not only means that the wide net cast by foreign intelligence agencies captures significant swaths of domestic data, but also seriously questions the ongoing legitimacy of the prevailing foreign intelligence paradigm, rooted in a disregard for the privacy rights of foreigners. In particular, the migration of political debate to the international stage and the focus on "individuals" who are neither "foreign powers" nor "agents" of terrorist groups suggests that the same hazards historically recognized in the domestic security context are present — and must be addressed — on the international stage.

Five Eyes on the World's Communications: A Global Problem with No Global Solution

Perhaps the most substantive legal check on CSE's surveillance capacities is the prohibition on "directing" its activities at Canadians and the requirement to minimize the impact of its activities on Canadians' privacy if their data is collected incidentally.[98] This approach is more effective as a rhetorical tool than at protecting Canadians' privacy.[99] Nor is it acceptable to ignore the privacy of non-Canadians. The prohibition on directing CSE activities at Canadian persons (defined as any person in Canada or Canadian abroad) expressly permits the targeting of communications *known* to include those of Canadians, while prohibiting the *purposive* targeting of Canadian individuals. For CSE, to direct at or target means "to single out."[100] In the traditional phone context, this means that if you are directing your wiretap at someone outside of Canada and that person phones a Canadian, that call is fair game as an incidental collection.[101] On digital networks, however, traffic routing is "all intermixed together," meaning that any mass-scale collection of foreign communications is guaranteed to include significant amounts of Canadian data.[102]

With respect to interception of private communications ("content"), CSE filters communications streams en masse at key Internet traffic points.[103] It likely uses metadata selectors or keywords (e-mail addresses, telephone numbers, IP addresses with a probability of foreignness) to scan all communications passing through its network filters; all hits are collected.[104] Other agencies filter both the designated "to/from" fields of communications *and* their text-based content ("about" communications), meaning that an e-mail, text, or Facebook message referencing a targeted phone number would be collected.[105] CSE's definition of metadata selectors in this context might be broad enough to include URLs, Facebook account identifiers, or document-authoring information, in which case these, too, would be hits if present in an e-mail text or attachment.[106] The minister only authorizes "classes of monitoring activities," so CSE selects targeting keywords and applies them to monitored communications streams by itself.[107] With respect to private communications incidentally acquired, CSE must minimize the impact on Canadians by expeditiously determining whether these are "essential" to foreign intelligence.[108] In 2013, sixty-six private communications of Canadians were retained for current and future use.[109] The number

likely does not represent discrete communications, but rather communications streams (all text messages between 613-555-5555 and <foreign number>).[110] Moreover, this only represents *retained* communications. The reported NSA 1:9 intake relevance ratio suggests that an additional 594 Canadian communications (streams) were collected, analyzed, and eventually discarded.[111] By comparison, the RCMP's extensive domestic mandate rested in its entirety on 700 intercepted communications in 2012.[112]

Metadata is not only collected and used to identify what content to collect, but increasingly for its own intelligence value. This is governed by different rules. CSE cannot "direct metadata analysis at Canadians" but, critically, the statutory obligation to expeditiously identify and delete Canadian data not deemed "essential" only applies to "private communications" (i.e., *not* metadata).[113] Instead, post-collection minimization procedures for metadata are anaemic, limited to suppressing identifying details of Canadians in derived intelligence reports.[114] Neither the deletion of metadata known to belong to Canadians,[115] nor the placement of meaningful restrictions on its analysis is required; CSE analysts can access Canadian metadata without even seeking senior management approval.[116]

It is clear CSE has a lot of Canadian metadata at its disposal. It adopts a permissive definition of "directed at Canadians" that allows extensive use of this metadata. One revealed CSE program in particular involved an analytical model designed to "track" individuals by correlating identifiers (Facebook and Google cookie IDs, e-mail addresses) associated with geolocated Wi-Fi network IP addresses.[117] A metadata packet timestamped at 11 a.m. containing "canuck@maple.ca" and an IP address known to be used by a particular cafe's Wi-Fi network is an accurate indicator of canuck's location. No metadata was collected for the program, meaning that the extensive underlying metadata set is indicative of CSE's regular holdings.[118] The program description notes that in one tested Canadian city over 300,000 active IDs associated with two sets of public Wi-Fi networks were identified in a short two-week period — a lot of Canadian metadata.[119] Despite the fact that the test program was clearly directed at people within Canada ("at Canadians"), its defenders argued it was not "directed at Canadians" because it did not "identify any individual Canadian."[120] This approach is inconsistent with the *Privacy Act* definition of personal information by which CSE claims to be bound, and which has been held to clearly apply to similar data

analytics.[121] If CSE does not consider this program to be "directed at Canadians," then there are few limits on the extensive analysis it can make of its Canadian metadata.[122]

This permissive approach to Canadian metadata is particularly problematic in light of CSE's access to FVEY resources. Active integration of CSE and other FVEY resources, including tasking intercept capacities and access to shared databases through interoperable interfaces has been underway since at least 2010.[123] Some CSE analytic programs make highly integrated use of FVEY metadata databases.[124] The FVEY agencies that create these databases are not legally prevented from targeting Canadians in their acquisition programs and, in fact, many operate under the assumption that their constitutional privacy obligations have no extraterritorial application. The databases and capacities in question are therefore generated without any legal obligation to respect the human rights of Canadians. When using these databases, CSE remains bound by the prohibition on "directing its activities at Canadians." However, with respect to metadata at least, CSE appears to consider it appropriate to analyze Canadian-rich datasets in its foreign intelligence programs. Moreover, CSE uses its entire metadata resources (inclusive of FVEY resources) when assisting domestically empowered agencies such as the RCMP and CSIS under its (c) mandate, without distinction as to how the underlying data was collected.[125] Recently introduced Bill C-51 seeks to dramatically expand this domestic element of CSE's activities by granting CSIS an open-ended digital disruption mandate, which will be implemented through CSE assistance, with all the FVEY resources at its disposal.[126]

This round robin — whereby each agency operates under no legal restrictions when spying on the citizens of its FVEY allies, and the spoils of the exercise are shared by all — raises a number of issues. While it is indisputable that privacy is an internationally recognized human right, FVEYs argue that their obligations to respect this right stop at their respective territorial borders. Additionally, some have argued that the context of foreign intelligence in particular operates as a categorical "exception" to privacy. On these bases, each FVEY agency deems itself free to spy on the world's communications networks as long as they do not target domestic citizens. Neither of these arguments is sustainable in the modern era. Digital communications networks are too intertwined for the status quo — where everything "foreign" is fair game — to continue.

While historical limitations on extraterritorial privacy obligations were steeped in principles of comity, the ability to spy on political leaders and citizens of allies without restriction does more to undermine than "facilitate interstate relations and global co-operation."[127] It also increasingly raises the same human rights implications on the international stage that have led to the strict regulation of national security surveillance domestically.[128] Resolution and debate of political issues increasingly happens on the global stage. The need for interoperability of digital networks is a particular driver for international resolution of domestic political issues at a range of supra-national governance bodies (Internet Governance Forum, Organization for Economic Co-operation and International Telecommunication Union).[129] Trade agreements increasingly address a range of domestic issues, and there are ongoing attempts to imbue new hemisphere-wide bodies with significant control over e-commerce.[130] Further, many domestic policy issues are now a matter of *integrated* international debate, as individuals from around the world discuss these matters on international online platform.[131] Even legal disputes are increasingly resolved on the international stage, where the historically permissive foreign intelligence approach permits states to spy on their legal adversaries.[132] There is evidence that the prevailing mass foreign surveillance model is already having a chilling effect on the ability of reporters and civil society advocates in both their domestic and international efforts.[133] It is also having an adverse impact on transborder data flows more generally, raising concerns regarding storage of data abroad.[134] All told, the "Wild West" approach to foreign surveillance is antithetical to comity in that it undermines "peaceable interstate relations and the international order" as well as the most fundamental of our democratic rights.[135]

The need for robust extraterritorial protection of human rights has been gaining significant attention in recent times. The Maastricht Principles open by noting that globalization has made territorial limits on human rights obligations inherently inconsistent with the universality of human rights, adopting a framework focused on state actors and causation with foreseeable impact as its primary touchstone.[136] With respect to communications surveillance specifically, there is growing recognition that current extraterritorial foreign intelligence surveillance is no longer consistent with human rights.[137] The High Commissioner on Human Rights in particular noted that granting minimal protection to "external communications"

constitutes impermissible discrimination in the application of human rights obligations to foreigners.[138] Technical acts of interception or data access abroad increasingly constitute exercises of effective control of the state's regulatory jurisdiction, implicating jurisdiction.[139] An unprecedented UN General Assembly resolution has now recognized that surveillance is having negative impacts on human rights "including extraterritorial surveillance and/or interception of communications."[140] Finally, the International Court of Justice issued an order prohibiting Australia from monitoring any communications between East Timor and its legal advisors regarding any proceedings before it.[141]

The right to privacy under the *Charter* has always protected *people* not *places*.[142] Canadian courts have recognized, however, practical and legal challenges in attempts to apply *Charter* standards to Canadian officials invoking foreign invasive state search powers abroad.[143] Requiring Canadian agents operating in another country to follow Canadian search and seizure standards could constitute a violation of sovereignty. Canadian agents are therefore typically permitted to follow foreign investigative standards when acting abroad. However, this rule is premised on two key assumptions: that Canadian agents operating abroad are restrained by *some* legal framework (that of the foreign country) and that Canadian courts retain some control through the ability to exclude evidence gathered abroad in a manner that is inconsistent with fundamental justice.[144] Neither applies here. CSE's foreign surveillance does not "rely on [foreign] state compulsion" to invade the privacy of foreign citizens — it neither operates under foreign laws nor is constrained by them.[145] As the fruits of its surveillance are rarely used in court, the threat of exclusion is non-existent. More importantly, however, the leeway granted to foreign investigations ends where violations of fundamental and internationally protected human rights begin.[146] By explicitly failing to account for foreigners' individual privacy rights *in any way at all*, CSE's legal framework fails to strike a proportionate balance and constitutes a violation of the right to privacy.[147] The *Charter* must constrain CSE's activities in some manner, as nothing else can. Notably, as a matter of comity, allowing CSE to disregard the privacy of foreign citizens implicitly allows all other states to disregard the privacy of our own.

CSE's participation in the FVEY network is more complex. Courts have recognized that the *Charter* does not apply to the

activities of foreign agencies assisting Canadian counterparts, nor is there any direct mechanism to compel foreign agencies to operate by *Charter* standards.[148] The *Charter* does apply, at minimum, to CSE participation in a process clearly violative of fundamental human rights, if there is a sufficient causal connection between CSE and the resulting violation.[149] FVEY resource sharing is highly integrated, with CSE likely able to directly task at least some FVEY monitoring resources.[150] Such direct tasking often requires no intervention or approval by the agency hosting the resource once general arrangements are in place, giving CSE practical control. CSE has repeatedly stated Canadian law binds its use of such capacities, if only with respect to the protection of Canadians.[151] Canadian law is therefore practically capable of restricting CSE use of FVEY resources. The FVEY cooperative is premised on a foundation of disregard for the privacy rights of foreigners and participants are not meaningfully constrained by their domestic laws.[152] Each time CSE tasks the FVEY network, it takes the risk that another agency will act independently on the information, leading to unconstitutional "detention or harm."[153] CSE has direct and explicit knowledge based on its own legal advice that tasking FVEY partners involves "the breach of international law by the requested second parties."[154] Canadian law should restrict CSE's use of these resources so as to respect the rights of non-Canadians.[155] Arguably, the *Charter* requires it.

While CSE cannot obligate its FVEY partners to adopt *Charter*-compliant information-gathering activities, it *can* more effectively constrain its own intelligence gathering and tasking of FVEY resources to reflect the privacy of affected targets. Those could include a reasonable grounds standard, for example, or the application of caveats.[156] It can also lead by example, or engage its allies in discussions geared towards an alliance that respects the privacy rights of all individuals.[157] However, domestic governments will not undertake such changes on their own initiative. Governments rarely act to curtail their own surveillance powers. As it will generally be politically palatable to placate domestic populations with reassurances that extraordinary powers are directed externally, there is an element of discrimination inherent in this system, which impacts minimally on voters.[158] The impetus for any form of effective change to this framework can only come from the *Charter* and the Courts entrusted with protecting the fundamental values enshrined within it.

Conclusion

The last decade has seen a dramatic expansion in the integration of communications networks, as well as in the portion of our daily lives that have become digital. Changes to the threat model and the operational approaches of foreign intelligence agencies have placed all of these interactions in the digital sphere within the unfettered and limitless scope of agencies whose legal frameworks were developed in a Cold War, spy-vs.-spy context that is categorically inapplicable to daily interactions of individuals, in Canada or abroad. The oversight of these entities, while important, has proven to be an ineffective check on the broad powers granted to CSE and its counterparts. At the same time, globalization and interconnectivity have moved the discussion of central political and democratic issues, once primarily in the domain of domestic politics, onto the international stage and within the granted purview of these agencies. Most importantly, the unprecedented scope of individual data collection these agencies have undertaken raises serious questions as to the underlying proportionality of the prevailing model and demands an urgent re-evaluation.

Notes

1. The New Transparency, "What Is IXmaps?," <https://vimeo.com/67102223>, at 1:56 minutes; Ron Deibert, "Why NSA Spying Scares the World," *CNN*, 12 June 2013, <cnn.com>.
2. Nick Hopkins, "The UK Gathering Secret Intelligence via Covert NSA Operation," *Guardian*, 7 June 2013, <http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>. ("… the service has been made available to spy organisations from other countries").
3. Brian Fung, "The NSA's Giant Utah Data Center Will Probably Hold a Bunch of Spam," *Washington Post*, 15 October 2013, <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/15/the-nsas-giant-utah-data-center-will-probably-hold-a-bunch-of-spam/>.
4. 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>.
5. Bill C-36, *Anti-Terrorism Act*, 2001, 1st Sess, 37th Parl, 2001 (as assented to 18 December 2001).
6. Privacy International, "Eyes Wide Open," Version 1.0, *Privacy International*, 26 November 2013, <privacyinternational.org>, at 38 *et seq*.

7. CSE operates under a tri-partite mandate: providing foreign intelligence to the government (its (a) or foreign intelligence mandate); providing advice and services aimed at protecting the government electronic infrastructure (its (b) or IT defence mandate); and providing technical/operational assistance to federal investigative agencies (its (c) or assistive mandate): *National Defence Act*, RSC 1985, c N-5, [NDA] at ss. 273.64(1)(a)-(c). This chapter focuses on CSE's (a) mandate, touching on its other mandates only tangentially. Jane Bailey, "Systemic Government Access to Private-Sector Data in Canada," (2013) 2:4 *Oxford Journals, International Data Privacy Law* 207.
8. Colin Freeze, "Former U.S. Spymaster Praises American Intelligence Oversight, but Envies Canadian System's 'agility'," *Globe and Mail*, 1 May 2014, <http://www.theglobeandmail.com/news/national/former-us-spymaster-praises-american-intelligence-oversight-but-envies-canadian-systems-agility/article18357209/>.
9. Cindy Cohn & Mark Jaycox, "NSA Spying: The Three Pillars of Government Trust Have Fallen," *EFF Deeplinks*, 15 August 2013, <eff.org>.
10. *Privacy Act*, RSC 1985, c P-21, ss 4, 7 and 8.
11. *R v TELUS Communications Co.*, [2013] 2 SCR 3 [*TELUS*], generally, and per Abella, J., at 4.
12. *Proceedings of the Standing Senate Committee on National Security and Defence*, 1st Sess., 38th Parl, No. 13 (13 June 2005), at 19–20; Canada, Office of the Communications Security Establishment Commissioner, *Annual Report 2006–2007*, May (Ottawa: Public Works and Government Services Canada, 2007), <http://www.ocsec-bccst.gc.ca/ann-rpt/2006-2007/ann-rpt_e.pdf> [OCSEC 2007], at 4: "… there is an ever-widening knowledge gap between the general public and evolving technologies."
13. [*Name Redacted by the Court*], 2011 US Dist LEXIS 157706, (US FISC, 2011)[FISC11], at 5, 33–34. The mis-characterization began in 2006: [*Name Redacted by the Court*], 2012 US Dist LEXIS 189344, (US FISC, 2012), at 2.
14. Upstream intercepts data from communications cables, PRISM obtains it from providers: Snowden Disclosure, "PRISM/US-984XN Overview," April 2013, <snowdenarchive.cjfe.org>, at 3. Collectively, they intake approximately 220 billion items of Internet [DNI] and telephone [DNR] metadata in a given month: Glenn Greenwald & Ewan 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>.
15. UPSTREAM harvests in-transit metadata and keeps it in a 30 day "buffer" for NSA analysts to query and decide what to keep ("content" buffers are 3 days): NSA, "XKEYSCORE," Snowden Disclosure, 25 February

2008, <snowdenarchive.cjfe.org>[XKS]. In 2011, 250 million data points were persistently retained: *FISC11*, *supra* note 13 at 36, footnote 24.

16. See *Jewel v National Security Agency*, Docket #: 4:08-cv-04373, Initial Complaint, 18 September 2008, <eff.org>. The *Jewel* complaint asserts similar facts regarding the same NSA Internet monitoring program that were ultimately uncovered by FISC in the 2011 decision (*supra* note 13).
17. *Canadian Security Intelligence Service Act (Can.)(Re)*, [2013] FTR 125 [*Re X* FC2013] aff'd in *X (Re)*, [2014] 377 DLR (4th) 735 [*Re X* FCA] leave to appeal granted, [2014] SCCA No 481.
18. *Re X* FC2013, *supra* note 17 at 1–2 and 37.
19. *Re X* FC2013, *supra* note 17 at 55.
20. *R v Hape*, [2007] 2 SCR 292 [Hape]; *Schreiber v Canada (Attorney General)*, [2002] 3 SCR 269 [Schreiber].
21. Wesley Wark, "Electronic Communications Interception and Privacy: Can the Imperatives of Privacy and National Security be Reconciled?," March 2012, <cips.uottawa.ca> [Wark] at 5.
22. Canada, OCSEC, *Annual Report 2010–2011*, June (Ottawa: Public Works and Government Services Canada, 2011), <ocsec-bccst.gc.ca> [OCSEC 2011], at 6.
23. Canada, OCSEC, *Annual Report 2007-2008*, May (Ottawa: Public Works and Government Services Canada, 2008), <ocsec-bccst.gc.ca> [OCSEC 2008], at 2-3.
24. *Supra* note 21 at 15.
25. Canada, CSE, "CSE Commissioner's Review of [Redacted] Activities [Redacted]," Response to *Access to Information Act* request, 30 December 2010, <https://cippic.ca/uploads/ATI-OCSEC-review_of_CSE_metadata_activities.pdf>, [Metadata Review] at note 8; *Re X* FC2013 *supra* note 17 at 70–74.
26. Canada, OCSEC, *Annual Report 2009-2010*, June (Ottawa: Public Works and Government Services Canada, 2010), <ocsec-bccst.gc.ca> [OCSEC 2010], at 4.
27. Canada, OCSEC, *Annual Report 2005–2006*, April (Ottawa: Public Works and Government Services Canada, 2006), <ocsec-bccst.gc.ca> [OCSEC 2006].
28. CBC News, "Project Levitation and Your Privacy," *CBC News*, 28 January 2015, <cbc.ca>, quoting Associate Minister of National Defence Julian Fantino; CSE, "Response from the Communications Security Establishment to CBC's Questions," *CBC News*, 28 January 2015, <https://documentcloud.org/documents/1509928-response-from-the-communications-security.html>.
29. OCSEC 2008, *supra* note 23. Prior to 2008, there were cryptic references to interpretive disagreements, with no details: *supra* note 21 at 15.
30. Canada, OCSEC, *Annual Report 2002–2013*, June (Ottawa: Public Works and Government Services Canada, 2013), <ocsec-bccst.gc.ca> [OCSEC 2013] at 25.

31. *Re X* FC2013, *supra* note 17.
32. *Re X* FC2013, *supra* note 17 at 53.
33. *Re X* FC2013, *supra* note 17 at 110–15.
34. Canada, OCSEC, *Annual Report 2008–2009*, June (Ottawa: Public Works and Government Services Canada, 2009), <ocsec-bccst.gc.ca> [OCSEC 2009].
35. NDA, *supra* note 7, section 273.65 governs CSE interception of private communications through ministerial authorizations. As CSE cannot invade constitutionally protected privacy expectations without lawful authority (*R v Collins*, [1987] 1 SCR 265 at 23) its privacy invasive activities that do not include interception can operate further to ministerial directives issued under section 273.62(3).
36. NDA, *supra* note 7, ss 273.62(3) and 273.66.
37. *Lyster v Attorney General of Canada*, BCSC File No T-796-14, Statement of Claim, 1 April 2014, <bccla.org>; *Clapper v Amnesty International USA*, 568 US __ (2015) (US Supreme Court).
38. *Hunter v Southam Inc*, [1984] 2 SCR 145 at 160–62 [*Hunter*]; *R v Vu*, [2013] 3 SCR 657 [*Vu*] at 46.
39. Craig Forcese, "A Tale of Two Controversies: Thoughts on CSEC's Headline Act(s)," *National Security Law Blog*, 16 October 2013, <http://craigforcese.squarespace.com/national-security-law-blog/2013/10/16/a-tale-of-two-controversies-thoughts-on-csecs-headline-acts.html>.
40. NDA, *supra* note 7, s 273.64(1)(a); OCSEC, "Frequently Asked Questions," 8 December 2014, <http://ocsec-bccst.gc.ca/new-neuf/faq_e.php>: "Establishing intelligence priorities is a prerogative of the executive arm of government."
41. *Canada (Minister of National Revenue) v Coopers and Lybrand Ltd*, [1979] 1 SCR 495 at 507–8: (Minister "governed by many considerations, dominant among which is the public interest and his duty as an executive officer of the government"); *Hunter*, *supra* note 38 at 162–65: (Commission guided by public policy and expediency).
42. *R v Grant*, [1993] 3 SCR 223 at 239–40; *R v Simmons*, [1988] 2 SCR 495 [*Simmons*] at 47.
43. *Simmons*, *supra* note 42 at 49 (lower privacy expectations at borders); *R v Tse*, [2012] 1 SCR 531 [*Tse*] at 18 (exigency); *Ruby v Canada (Solicitor General)*, [2002] 4 SCR 3 [*Ruby*] at 40, 44; *Charkaoui v Canada (Citizenship and Immigration)*, [2007] 1 SCR 350 at 27.
44. *Simmons*, *supra* note 42 at 50–51: (warrantless searches must be less intrusive, based on specific grounds, and challengeable "before any person can be searched"); *Tse*, *supra* note 43 at 84–85; *Ruby*, *supra* note 43 at 42.
45. *Mahjoub (Re)*, 2013 FC 1096, [*Mahjoub*] at 32-34, 38-39; *Atwal v Canada*, [1988] 1 FCR 107 (FCA)[*Atwal*] at 35, 45-46; *Re X* FCA, *supra* note 17 at

86–87; *Re X* FC2013, *supra* note 17 at 99–100; *United States v US District Court*, 407 US 297 (1972) (US Supreme Court) [US 1972] (domestic security surveillance cannot be sole discretion of executive branch of government).

46. Senate, "Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the *Anti-Terrorism Act*" (February 2007) [Senate 2007] at 77: ("warrants from Canadian courts have no jurisdiction outside of Canada"). <http://www.parl.gc.ca/Content/SEN/Committee/391/anti/rep/repo2feb07-e.pdf>.
47. Bill C-44, *Protection of Canada from Terrorists Act*, SC 2015, c. 9, April 23, 2015, at 8(2).
48. This reform is a direct response to *Re X* FC2013, *supra* note 17.
49. *Mahjoub*, *supra* note 45.
50. *NDA*, *supra* note 7 at 273.65.
51. *Vu*, *supra* note 38 at 47.
52. Senate 2007, *supra* note 46 at 78, Recommendation 18.
53. *Atwal*, *supra* note 45 at 24, 35–36.
54. *Atwal*, *supra* note 45 at 35.
55. OCSEC 2008, *supra* note 23 at 4; OCSEC 2010, *supra* note 26 at 4.
56. Authorizations are valid for up to twelve months, typically renewed annually (NDA, *supra* note 7 at s 273.68). In 2014 the six long-standing authorizations were "reformatted" into three (without any corresponding substantive changes): Canada, OCSEC, *Annual Report 2013–2014*, June (Ottawa: Public Works and Government Services Canada, 2014) [OCSEC 2014], at 39.
57. OCSEC 2008, *supra* note 23 at 4.
58. Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2 July 2014) [PCLOB FAA702], at 7. Open Rights Group, "GCHQ and Mass Surveillance," *OpenRightsGroup.org*, 11 March 2015, <https://www.openrightsgroup.org/ourwork/reports/gchq-and-mass-surveillance>, at 6–8.
59. *Re X FC2013*, *supra* note 17 at 55, 105. EONBLUE is CSE's primary interception program: CSE, "CSEC SIGINT Cyber Discovery: Summary of Current Effort," *Snowden Disclosure*, November 2010, <snowdenarchive.cjfe.org> [Cyber Discovery], at 13–14. EONBLUE is an "XKEYSCORE" input (*Ibid*., at 18), an NSA-developed resource allowing interoperability in intercept, search, and storage capacities across FVEY agencies: XKS, *supra* note 15. See also Christopher Parsons, "Canadian SIGINT Summaries," *Technology, Thoughts & Trinkets*, 6 February 2015, <https://christopher-parsons.com/writings/cse-summaries/> [Parsons].
60. Siobhan Gorman & Jennifer Valentino-Devries, "New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's

Traffic, Can Snare Emails," *Wall Street Journal*, 30 August 2013: "The NSA defines access as 'things we actually touch,'… telecom companies do the first stage of filtering … based on the NSA's criteria." <http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470>.

61. OCSEC 2014, *supra* note 56 at 40. *X, Re*, [2010] 1 FCR 460 [*Re X* FC2009] at 58 suggests an "interception" occurs when the "substantive content of the communication" is acquired in Canada, not when it is otherwise processed in a redacted manner abroad.
62. *R v Kang-Brown*, [2008] 1 SCR 456 (dog sniffing luggage indicates whether bag does or does not contain drugs constituting a search). *TELUS*, *supra* note 11.
63. Metadata Review, *supra* note 25 at 5: "Metadata is not [redactions] a private communication."
64. Greg Weston, "Spy Agency CSEC Needs MPs' Oversight, Ex-Director Says," *CBC News*, 7 October 2013, <http://www.cbc.ca/news/politics/spy-agency-csec-needs-mps-oversight-ex-director-says-1.1928983>.
65. Tamir Israel, "Rogers' Use of Deep Packet Inspection Equipment," *CIPPIC*, 2 December 2009, <cippic.ca>, at 14–16.
66. *ACLU v. Clapper*, Case No. 14-42, *Amici Curiae* Brief of Experts in Computer and Data Science, 13 March 2014, (US 2nd Cir 2014).
67. *Criminal Code*, RSC 1985, c C-46, recently enacted section 487.011(c) defines "transmission data" as data that "does not reveal the substance, meaning or purpose of the communication." CSE does not include this caveat: Metadata Review, *supra* note 25 at 10.
68. CSE, "LEVITATION and the FFU Hypothesis," *Snowden Disclosure*, <snowdenarchive.cjfe.org> [LEVITATION], at 5–6 (URLs), 15 (FacebookID), 3 (search term analytics); XKS, *supra* note 15 at 17 (document-authoring information).
69. *R v Spencer*, [2014] 2 SCR 212 at 45–47, 50 (Online identifiers attract high expectations of privacy where revealing otherwise anonymous online activities).
70. Metadata Review, *supra* note 25 at 16.
71. Spencer Ackerman & James Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ," *The Guardian*, 28 February 2014, <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> [OPTICNERVE].
72. *Ibid.* See also Matt Kwong, "Samsung SmartTV an 'Absurd' Privacy Intruder," *CBC News*, 10 February 2015, <http://www.cbc.ca/news/technology/samsung-smarttv-an-absurd-privacy-intruder-ann-cavoukian-says-1.2950982>.
73. Barton Gellman, Julie Tata & Ashkan Soltani, "In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are," *The*

Washington Post, 5 July 2014) [Gellman], <http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html>.

74. Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," 23 January 2014, [PBCLOB 215] at 28–29, 60–65.
75. *Ibid.* at 61–63.
76. Scott Shane, "No Morsel Too Miniscule for All-Consuming NSA," *New York Times*, 2 November 2013, <http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html> [Shane].
77. *NDA*, *supra* note 7 at s. 273.61.
78. *Supra* note 21 at 9; *Proceedings of the Standing Senate Committee on National Security and Defence*, 2nd Sess, 41st Parl, No 2 (3 February 2014) [Senate 2014] at 41, 66. <http://www.parl.gc.ca/content/sen/committee/412/SECD/pdf/02issue.pdf>.
79. Glenn Greenwald, "Documents from No Place to Hide," *GlennGreenwald.net*, <http://glenngreenwald.net/#BookDocuments>, at 95–96.
80. James Cox, "Canada and the Five Eyes Intelligence Community," *Strategic Studies Working Group Papers* (18 December 2012) [Cox], at 7.
81. Senate 2014, *supra* note 78 at 38.
82. Canada, SIRC, "Bridging the Gap: Recalibrating the Machinery of Security Intelligence and Intelligence Review," *Annual Report 2012–2013* (Ottawa: Public Works and Government Services Canada, 2014) [SIRC 2013], at 20.
83. Senate 2014, *supra* note 78 at 38.
84. Colin Freeze & Stephanie Nolen, "Charges That Canada Spied on Brazil Unveil CSEC's Inner Workings," *Globe and Mail*, 7 October 2013, <http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/>; Greg Weston et al., "New Snowden Docs Show US Spied during G20 in Toronto," *CBC News*, 1 December 2013, <http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448>; Ewen MacAskill et al., "GCHQ Intercepted Foreign Politicians' Communications at G20 Summit," *Guardian*, 17 June 2013, <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>; David Sanger & Thom Shanker, "NSA Devises Radio Pathway into Computers," *New York Times*, 14 January 2014, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html; NSA, "Intro to the VPN Exploitation Process," *Snowden Disclosure*, 13 September 2010, <snowdenarchive.cjfe.org>, at 40; Ryan Gallagher, "Operation Socialist," *The Intercept*, 12 December 2014, <firstlook.org>.

NSA, "UN Climate Change Conference in Copenhagen — Will the Developed and Developing World Agree on Climate Change?" *Snowden Disclosure*, 7 December 2009, <snowdenarchive.cjfe.org>.

85. Shane, *supra* note 76.
86. Jean-Pierre Plouffe, "Statement by CSE Commissioner the Honourable Jean-Pierre Plouffe re: January 30 CBC Story," *Office of the CSE Commissioner*, 31 January 2014, <ocsec-bccst.gc.ca>. (CSE can use domestic metadata to conduct analytical experiments); OPTICNERVE *supra* note 71 (GCHQ experiments with intercepted video chats to improve facial recognition).
87. *US* 1972, *supra* note 45: "History abundantly documents the tendency of Government… to view with suspicion those who most fervently dispute its policies." <http://openjurist.org/407/us/297>.
88. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UNHRC, 23rd Sess, UN Doc A/HRC/23/40 (2013) [*La Rue*], <ohchr.org>: "The concept is broadly defined and is thus vulnerable to manipulation by the State."
89. *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia)*, Order of March 3, 2014 [*Timor-Leste*].
90. Canada, SIRC, "Reflections," Security Intelligence Review Committee, Ottawa, 2005, <sirc-csars.gc.ca>, at 7.
91. Colin Freeze, "Spy Agency's Work with CSIS, RCMP Fuels Fears of Privacy Breaches," *Globe and Mail*, 31 January 2014, <http://www.theglobeandmail.com/news/politics/spy-agencys-work-with-csis-rcmp-fuels-fears-of-privacy-breaches/article16623147/>.
92. The NSA's statutory obligation to direct its activities only at "foreign powers and their agents" was removed: Tamir Israel, Katitza Rodriguez, & Mark Rumold, "U.S. Foreign Intelligence: From Carte Blanche Surveillance to Weak [Domestic] Protections," *EFF Deeplinks*, 15 June 2013, <eff.org/>.
93. NSA, "Content Extraction Enhancement for Target Analytics," *Snowden Disclosure*, 9 June 2011, <snowdenarchive.cjfe.org>, at 8.
94. Glenn Greenwald & Murtaza Hussain, "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On," *The Intercept*, 9 July 2014, <firstlook.org>.
95. Luke Harding, "Edward Snowden: US Government Spied on Human Rights Workers," *Guardian*, 8 April 2014, <http://www.theguardian.com/world/2014/apr/08/edwards-snowden-us-government-spied-human-rights-workers>.
96. Jonathan Easley, "Snowden: NSA Targeted Journalists Critical of Government After 9/11," *The Hill*, 13 August 2013, http://thehill.com/blogs/blog-briefing-room/news/316751-snowden-nsa-targeted-journalists-critical-of-government-after-911.

97. Mark Schone et al., "Snowden Doc Shows UK Spies Attacked Anonymous Hackers," *NBC News*, 5 February 2014, <http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361>.
98. *NDA*, *supra* note 7 at s 273.64(2).
99. Michael Geist, "Why Better Oversight Won't Fix Internet Surveillance and the New Anti-Terrorism Bill," *MichaelGeist.ca*, 10 February 2015, <michaelgeist.ca> [Geist].
100. Metadata Review, *supra* note 25, at footnote 17: "To target (verb) means: "To single out [redactions]."
101. Senate 2014, *supra* note 78 at 63.
102. *Ibid.* at 71. PCLOB FAA702, *supra* note 58 at 7 (MCT); Gellman, *supra* note 73; Geist, *supra* note 99.
103. EONBLUE monitors communications streams for keywords at backbone data speeds: Cyber Discovery, *supra* note 59 at 13–14. Parsons, *supra* note 59.
104. CSE has confirmed it uses metadata in part to help it target non-Canadians in its content acquisition programs: OCSEC 2014, *supra* note 56 at 21. Content is also buffered for three days, and it remains unclear whether buffers are generated before or after the targeting criteria are applied.
105. PBCLOB FAA702, *supra* note 58 at 7.
106. *Supra* note 68.
107. After it had proven impossible to properly restrain NSA analyst searches, FISC recently mandated prior judicial approval for any search selectors to be used on one of its telephone metadata databases: PCLOB 215, *supra* note 74 at 52.
108. *NDA*, *supra* note 7 at s 273.65(2)(d).
109. OCSEC 2014, *supra* note 56 at 66.
110. PCLOB FAA702, *supra* note 58 at 39–41 (Internet transactions not discrete communications).
111. Gellman, *supra* note 73.
112. Canada, "2013 Annual Report on the Use of Electronic Surveillance," (Ottawa: Public Safety Canada, 2014), at Table 7.
113. *NDA*, *supra* note 7 at s. 273.65(2)(d), only applies to "the interception of private communications." CSE does not consider this to include metadata (*supra* note 63).
114. Metadata Review, *supra* note 25 at 5, footnote 7.
115. Senate 2014, *supra* note 78 (CSE Chief John Foster), at 71: "We will keep [all collected] metadata… If it is Canadian, then we… make sure we protect the privacy of that information and how we use it."
116. Metadata Review, *supra* note 25 at 5.
117. Greg Weston et al., "CSEC Used Airport Wi-Fi to Track Travellers," *CBC News*, 30 January 2014, <http://www.cbc.ca/news/politics/

csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>; Bruce Schneier, "CSEC Surveillance Analysis of IP and User Data," *Schneier on Security*, 3 February 2014, <schneier.com>.

118. Senate 2014, *supra* note 78 at 54–55: "It's part of our normal global collection."
119. CSE, "IP Profiling Analytics & Mission Impacts," *Snowden Disclosure*, 10 May 2012, <http://cbc.ca/news2/pdf/airports_redacted.pdf>, at 4, 23.
120. Senate 2014, *supra* note 78 at 56.
121. The *Privacy Act* definition of "identifiable Canadian individual" that CSE uses (OCSEC 2014, *supra* note 56 at 42) applies to the type of large scale analytics demonstrated here because the identifiers (IP addresses, etc.) at the heart of the program are traceable back to an individual: PIPEDA Report of Findings #2009-010, September 2009, at 47–49; Office of the Privacy Commissioner of Canada, "Policy Position on Behavioural Advertising," *OPC Guidelines*, 6 June 2012); Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports* 3:1376 (25 March, 2013), <http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html>.
122. An active CSE program that analyzes metadata to identify individuals who have viewed certain documents on file upload sites includes Canadian outputs, anonymized in the subsequent intelligence reports, but not in the underlying database: LEVITATION, *supra* note 68 at 12.
123. LEVITATION, *supra* note 68 at 18.
124. LEVITATION, *supra* note 68 at 15 uses MARINA, an NSA metadata database, to query Facebook IDs.
125. Metadata Review, *supra* note 25, at 15, second bullet. *Re X* FC2013, supra note 17.
126. Bill C-51, *Anti-Terrorism Act*, 2015, 2 Sess, 41st Parl, 2015 (1st reading) (30 January 2015) at Clauses 42–44.
127. *Hape*, *supra* note 20 at 50. Laura Poitras et al., "A is for Angela: GCHQ and NSA Targeted Private German Companies and Merkel," *Der Spiegel*, 29 March 2014, <spiegel.de>; Canadian Press, "Harper 'Very Concerned' about Reports of Canada Spying on Brazil," *Toronto Star*, 8 October 2013, <http://www.thestar.com/news/world/2013/10/08/harper_very_concerned_about_reports_of_canada_spying_on_brazil.html>.
128. *Hape*, *supra* note 20 at 51.
129. Milton Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Boston: MIT Press, 2002); Jeremy Malcolm, "The Role of Governments in Internet Governance," *Consumers International*, 28 May 2013, <http://www.diplomacy.edu/sites/default/files/May%202013%20IG%20webinar%20PDF%20-%20Dr%20Jeremy%20Malcolm.pdf>.
130. Maira Sutton, "It Doesn't Matter Who Does the Lobbying: Trade Agreements Aren't the Place for Internet Regulations," *EFF Deeplinks*,

19 December 2014, <eff.org>; Jane Kelsey & Burcu Kilic, "Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality," *PSI* (17 December 2014), <http://www.world-psi.org/sites/default/files/documents/research/briefing_on_tisa_e-commerce_final.pdf>.

131. Nahed Eltantawy & Julie West, "Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory" (2011) 5 *International Journal of Communication* 1207; Hillary Rodham Clinton, US Secretary of State, "Remarks on Internet Freedom" *US Department of State*, 21 January 2010, <state.gov>.
132. *Timor-Leste*, *supra* note 89.
133. Human Rights Watch, "With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law and American Democracy," *Human Rights Watch*, (July 2014): 22–23; <http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf>; and Access et al., "Letter to General Keith Alexander and the Honorable Michael Froman,"12 November 2013, <http://www.consumerfed.org/pdfs/cso-letter-on-nsa-surveillance-11-12-13.pdf>.
134. Parliament of the European Union, "Inquiry on Electronic Mass Surveillance of EU Citizens," *Committee on Civil Liberties, Justice and Home Affairs (LIBE)* (2013–2014), <http://europarl.europa.eu/document/activities/cont/201410/20141016ATT91322/20141016ATT91322EN.pdf>, at 46–47; Claire Cain Miller, "Revelations of NSA Spying Cost US Tech Companies," *New York Times*, 21 March 2014, <http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>.
135. *Hape*, *supra* note 20 at 50–52.
136. Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights, (28 September 2011), Principles 8(a) and 9(b).
137. La Rue, *supra* note 88 at 64; International Principles on the Application of Human Rights to Communications Surveillance, (July 2013) Final Version, *Necessary and Proportionate*, <https: necessaryandproportionate.org>, [IPAHRCS].
138. UN High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," UNHRC, 27th Sess., UN Doc A/HRC/27/37 (2014) [High Commissioner], at 36.
139. *Ibid.* at 34–35.
140. "The Right to Privacy in the Digital Age," GA Res 68/167, UNGAOR, 68th Sess, UN Doc A/RES/68/167; Colum Lynch, "Inside America's Plan to Kill Online Privacy Rights Everywhere," *Foreign Policy*, 20 November 2013, <foreignpolicy.com>; Ewen MacAskill & James Ball, "UN Surveillance Resolution Goes Ahead Despite Attempts to Dilute Language," *The*

Guardian, 21 November 2013, <http://www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language>.

141. *Timor-Leste*, *supra* note 89 at 52.
142. *Hunter, supra* note 38 at 159; *Hape*, *supra* note 20 at 94, 159–61.
143. *Hape*, *supra* note 20.
144. *Ibid.* at 111–12, 169.
145. *Hape*, *supra* note 20 at 74, 160–74, *Canadian Security Intelligence Service Act (Re)*, [2008] 4 FCR 230 at 51.
146. *Ibid.* at 52; *Canada (Justice) v Khadr*, [2008] 2 SCR 125 at 18 [*Khadr08*]; *Canada (Prime Minister) v Khadr*, [2010] 1 SCR 44 [*Khadr10*].
147. *Hape*, *supra* note 20 at 100.
148. *Hape*, *supra* note 20 at 112.
149. *Khadr08*, *supra* note 146 at 18; *Khadr10*, *supra* note 146 at 14, 19; *Hape*, *supra* note 20 at 52, 175.
150. Likely including direct access to existing databases as well as capacity to directly send keywords to some FVEY network monitoring equipment: *supra* notes 59 and 124. Contrast *Hape*, *supra* note 20 at 74.
151. *Cox*, *supra* note 80 at 7.
152. *Re X* FC2009, *supra* note 61 at 77.
153. SIRC 2013, *supra* note 82 at 19.
154. *Re X* FC2013, *supra* note 17 at 105; *Khadr10*, *supra* note 146, at 20, 24; *Wakeling v United States of America*, 2014 SCC 72 at 80.
155. *Hape*, *supra* note 20 at 46 and 169; *Timor-Leste*, *supra* note 89.
156. *Supra* notes 53, 54; IPAHRCS, *supra* note 137; High Commissioner, *supra* note 138 at 21 *et seq.* and note 14.
157. High Commissioner, *supra* note 138 at 33; *Hape*, *supra* note 20 at 112.
158. High Commissioner, *supra* note 138 at 36.

Page left blank intentionally