CHAPTER IV

Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State

Lisa M. Austin

Introduction

The Snowden revelations have revealed to us, with impressive documentation, the technical infrastructure of contemporary state surveillance. What is less obvious, but of great importance, is the revelation of the legal infrastructure of this surveillance. In this chapter I argue that this infrastructure is best understood as one of "lawful illegality."

One aspect of the lawful illegality of surveillance is the conflicting reactions of citizens and authorities when surveillance programs are revealed. Members of the public, upon learning what some national security authority is doing, protest that it must be illegal. The national security authority, and government, claim that everything they do is lawful. The label "lawful illegality" captures this conflict between the perspective of the state and the perspective of ordinary citizens.

It is likely the case that spy craft has always operated within a space of conflicted legality. For example, state security agencies might have lawful authority under their domestic law to engage in actions abroad that might breach the domestic laws of other nations or international legal norms.[1] But what has become so clear in the wake of the Snowden revelations is the dramatically changed landscape of state surveillance. Ideas of what is included in "national security"

have broadened, and targets now include ordinary individuals and not simply foreign states and foreign agents. The line between criminal offences and national security offences has blurred, both domestically and internationally. Effective state action against terrorism requires cooperation between national security authorities, law enforcement authorities, and border officials, both within a state and across borders, as well as sophisticated technologies that make use of a global and interconnected communications infrastructure.[2] This changed landscape reveals a deeper tension than simply conflicting perspectives of legality. My claim in this chapter is that there is a serious rule of law problem.

The rule of law requires the commitment that state action itself be subject to the law. In this chapter I claim that the issues of secrecy, complexity, and jurisdiction work together to create "lawful" paths for state surveillance for national security purposes that are nevertheless in deep tension with a general commitment that this surveillance be subject to the oversight and accountability demanded by the rule of law. Throughout, I illustrate these issues with a set of examples largely taken from the Snowden revelations, with a Canadian perspective. These examples are not meant to provide an exhaustive overview of the issues, but to highlight the importance of attending to these larger questions of legality if we are going to move forward and design a better system of oversight.

Illegality and Emergencies

In the aftermath of 9/11, there was a significant rule-of-law debate regarding the role of law in fettering executive discretion in times of emergency. This framework of "emergencies" remains important in public discourse concerning surveillance. For example, United States Supreme Court Justice Scalia commented upon the possibility that the Supreme Court would ultimately decide upon the constitutionality of some of the American surveillance programs.[3] The legal question, he said, is about "balancing the emergency against the intrusion [on the individual]." He also suggested that the court was the "least qualified" institution to decide this issue. This lack of expertise, one can infer, concerns the court's qualification to judge the demands of emergencies, not the demands of the Fourth Amendment; whatever judgment emergencies require, the executive and not the courts are the experts.

As David Dyzenhaus has argued, some of the post-9/11 debate regarding emergencies and the rule of law concerns the different responses one might take to the existence of either legal black holes or legal grey holes. A black hole is where the legislature seeks to carve out a space of no-law; a grey hole is "one in which there is the facade or form of the rule of law rather than any substantive protections."[4] The space created by such holes is a space for executive discretion and the need for such space derives from the perceived exceptional nature of national emergencies, where it is difficult to anticipate in advance what that emergency will be and how one should respond.[5]

This framework of emergencies, with its themes of uncertainty and unenforceability, is both helpful and unhelpful when applied to state surveillance. It is helpful in that the exceptional nature of terrorism has deeply influenced contemporary methods of state surveillance. One aspect of the exceptional nature of terrorism is indeed its unpredictability. It is difficult to anticipate who will engage in acts of terrorism: agents of foreign powers, members of existing and known terrorist organizations, affiliates abroad, or homegrown extremists? It is difficult to anticipate where an attack will take place, whether many civilians will be at risk, the potential scale of an attack, and so on. Another aspect of the exceptional nature of terrorism is the type of risk it is seen to be — not just a risk of potentially catastrophic harm, but a deep political threat to the state. For example, the United States considers itself to be at "war" against al-Qaeda.[6] The extraordinary nature of the threat of terrorism also underpins the US response of seeking to prevent future terrorist attacks, with a "never again" mentality.[7]

However, focusing on the exceptional nature of emergencies can distract us from the most salient features of the state surveillance methods Snowden has revealed to the world: they are in fact a rational, systematic, planned response to the perceived need to prevent terrorist attacks. In other words, the framework of emergencies concerns whether what is needed is a discretionary space for executive authority — either legal black holes or legal grey holes — to nimbly respond to exceptional circumstances that cannot be foreseen in advance. But state surveillance premised on the idea of collecting the "haystack" to find the "needle" is not about preserving discretion at all. It is about applying rational analytic methods to the problem of preventing certain kinds of threats that have been identified at least at some level of generality (e.g., terrorist threat).[8] The proper frame

of the rule of law challenge is not about the question of whether executive discretionary authority in relation to emergencies can and should be constrained by the reason of the law; instead, it is about whether mass surveillance as a mode of rational social ordering is in conflict with the deepest commitments of law as a mode of rational social ordering.

When we talk about the legality of surveillance, therefore, we need to focus less on the spaces of discretion and more on the systematic features of surveillance that put strain on our traditional understandings of the rule of law. In particular, I want to flag three issues. The first is the issue of secrecy and the degree to which it is demanded by the national security context. My claim is that it creates pressure for unilateral, rather than objective and public, interpretations of the law. The second is the issue of legal complexity, especially as it relates to law reform initiatives. Where there is an increased blurring between regular law enforcement, border control, and terrorism investigations, as well as increasingly complex relationships between private sector communications intermediaries and the state, gaining a clear public understanding of proposed changes to lawful access laws or the full significance of legal cases before the courts is extremely difficult. The third is the issue of jurisdiction and the extent to which national boundaries and questions of status (like citizenship) affect the lawfulness of surveillance. In particular, I argue that instead of providing us with the tools for accountability, status and jurisdiction allow for the leveraging of national boundaries to create an international surveillance regime with questionable accountability.

Secrecy and Unilateralism

One of the most basic understandings of the rule of law is that government itself is subject to law. As already noted, one of the remarkable things about the Snowden revelations is that the response of both the intelligence agencies and the governments involved has largely been to claim that they are acting in a lawful manner. What has become clear, however, is that these claims of lawfulness are often unilateral in the sense that they are either claims of a one-sided interpretation of the law or claims of deference to that one-sided interpretation within an accountability framework that is structurally biased. Secrecy is a key ingredient to this unilateralism. However, such unilateralism lies in tension with our deeper commitments to

legality, which demands that law reflect a "public" perspective and not that of an entity who is supposed to be regulated by that law.

In Canada, the Communications Security Establishment's claims of the lawfulness of its metadata program, for example, turn out largely to be a claim that there is a plausible legal interpretation that shows CSE's activities to be both within its statutory authority and consistent with the Canadian *Charter of Rights and Freedoms*. The problem is that the plausible legal interpretation is one provided by the government itself and its conclusion of lawfulness is far from obvious to an outside observer. As we have seen from the public controversy surrounding the disclosures regarding CSE's alleged collection of communications metadata at public Wi-Fi spots, many well-informed commentators express incredulity regarding how such activities are lawful under either the *National Defence Act* or the Canadian *Charter of Rights and Freedoms*.[9]

CSE does not make its legal interpretation public, so its claims of lawfulness rest not just on its own legal interpretation but, importantly, on a secret interpretation. CSE itself often points to the independent oversight of the CSE commissioner as part of the accountability framework within which it operates.[10] This suggests that the CSE commissioner is able to independently assess the lawfulness of CSE's activities. However, we know from the annual reports of past CSE commissioners that where there is a difference of views regarding legal interpretation, it is CSE's view that prevails. For example, in his 2005–2006 annual report, Commissioner Lamer stated,

> With respect to my reviews of CSE activities carried out under ministerial authorization, I note that I concluded on their lawfulness in light of the Department of Justice interpretation of the applicable legislative provisions. I have pointed out elsewhere that there are ambiguities in the legislation as now drafted, a view that I share with my predecessor, the Hon. Claude Bisson, O.C., a former Chief Justice of Quebec. Currently, two eminent lawyers, the Deputy Minister of Justice and my independent Legal Counsel disagree over the meaning of key provisions that influence the nature of the assurance that I can provide.[11]

Similar statements have been made by subsequent commissioners.[12] Without an accountability mechanism that allows for the government's interpretation of the law to effectively be contested as well

as for a final determination by an objective body, like a court, then "lawfulness" turns out to simply mean a claim to operate within one's own interpretation of the law. Oversight, on this model, means independent assurance that one's activities conform to one's own interpretation of the law. To be subject merely to one's own interpretation of the law looks a lot like getting to be one's own judge, and it lies in deep tension with the ideal of law as an objective constraint on state power.

This unilateralism is exacerbated by several other layers of secrecy that remove a number of potential informal constraints that can operate to ensure balanced, rather than biased, legal advice. People seek legal advice because they want to do things and need to find out how to do them legally. There is a natural pressure, in such a context, to provide a permissive interpretation of the law. Many factors typically operate to provide a countervailing pressure, but most of these depend upon the understanding of the parties involved that the actions taken pursuant to that legal advice will be public and can be called into question by those affected by them. If there is reason to think that those affected can argue that the actions taken are in fact contrary to law, then there is a risk of legal liability that will factor into the original advice offered. More generally, public scrutiny through the press and academia provides another set of informal constraints, albeit less direct. But state surveillance operations, both in terms of general programs and in terms of particular operations, are secret. If surveillance is secret, then the people likely affected by the surveillance are in no position to contest it, and this removes one of the informal constraints that can operate to provide balance in determining the lawfulness of the surveillance. In other words, the layers of secrecy surrounding state surveillance structurally enable one-sided legal advice.

If the legal opinions establishing lawfulness are secret, if the activities at issue are secret, if the legal opinions are ones that even those tasked with oversight must defer to, then the "lawfulness" of surveillance is very one-sided indeed. The systematic effect of this on civil liberties should not be underestimated. David Cole has argued, for example, that post-9/11 civil society groups have been one of the most important guardians of constitutional and rule-of-law values, and not the more "formal mechanisms of checks and balances" in the United States.[13] Such groups cannot perform this function when they have no way of knowing the legal opinions and actions of the state, apart from what they learn from whistle-blowers.

We also need to view this unilateralism in the context of what two different whistle-blowers have told us about how the government might in different ways exert pressure for favourable legal interpretations.

The first whistle-blower is Edgar Schmidt, a retired Justice Department lawyer who is taking the Canadian government to court, seeking a declaration regarding what he considers to be unlawful practices in relation to the Department of Justice's review of proposed legislation and regulations. In his statement of claim, he argues,

> Since about 1993, with the knowledge and approval of the Deputy Minister, an interpretation of the statutory examination provisions has been adopted in the Department to the effect that what they require is the formation of an opinion as to whether any provision of the legislative text being examined is manifestly or certainly inconsistent with the Bill of Rights or the Charter and, in the case of proposed regulations, whether any provision is manifestly or certainly not authorized by the Act under which the regulation is made.[14]

This has yet to be tested in court. However, these allegations highlight some of the ways in which institutional cultures can develop in a manner that promotes, not bad faith interpretative practices, but at least a practice of "sharp elbows," where legal interpretation is routinely pushed as far as possible in the government's favour.[15]

The other whistle-blower is Edward Snowden. In a statement to the European Parliament, Snowden outlined the National Security Agency's (NSA) role in law reform in Europe. His remarks are worth quoting at length:

> One of the foremost activities of the NSA's FAD, or Foreign Affairs Division, is to pressure or incentivize EU member states to change their laws to enable mass surveillance. Lawyers from the NSA, as well as the UK's GCHQ, work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. These efforts to interpret new powers out of vague laws is an intentional strategy to avoid public opposition and lawmakers' insistence that legal limits be respected, effects the GCHQ internally described in its own documents as "damaging public debate."

> In recent public memory, we have seen these FAD "legal guidance" operations occur in both Sweden and the Netherlands, and also faraway New Zealand. Germany was pressured to modify its G-10 law to appease the NSA, and it eroded the rights of German citizens under their constitution. Each of these countries received instruction from the NSA, sometimes under the guise of the US Department of Defense and other bodies, on how to degrade the legal protections of their countries' communications. The ultimate result of the NSA's guidance is that the right of ordinary citizens to be free from unwarranted interference is degraded, and systems of intrusive mass surveillance are being constructed in secret within otherwise liberal states, often without the full awareness of the public.[16]

We have no evidence so far that Canada has been subject to such pressure, but Snowden's remarks highlight another cause for concern regarding secrecy and the unilateralism it enables — that a strategy of promoting legal interpretations enabling surveillance, rather than seeking to clarify the law through law reform, might be a strategy of actually avoiding public debate. The result is a claim of "lawfulness" that has not just lost its connection to the public point of view, but has sought to actively sever it.

Complexity and Lawful Access

In addition to secrecy, and sometimes working in conjunction with it, legal complexity undermines accountability. One aspect of this complexity, within Canada, is the different institutions that deal with national security concerns, including the RCMP, Canadian Security Intelligence Service (CSIS), and CSE. Oversight of each is handled differently, with limited ability to coordinate between oversight bodies even in relation to the ways in which these bodies cooperate and assist one another.[17] However, the complexity that I want to highlight here concerns law reform itself, given these interrelationships. That is, even if the state pursues public law reform rather than secret legal interpretations, it is often difficult to understand the full implications of legal changes. Instead of understanding themselves as participants in an open, transparent, and public debate, lawyers concerned about civil liberties need to approach proposed legislation with a "hacker" mentality, looking for non-obvious ways to read the

legislation in order to locate the little-understood legal vulnerabilities the government might exploit behind its wall of secrecy and protective official statements.

For example, Canada's ongoing debates regarding lawful access reform generally focus on the ordinary law enforcement context, and yet this reform has difficult-to-understand implications for surveillance in the national security context as well.

Since 9/11, the federal government has sought to pass lawful access legislation. One of the more recent failed iterations, Bill C-30, would have created a mandatory warrantless access regime for some kinds of metadata. In particular, both CSIS and Canadian police services could designate particular individuals who would be authorized to require any telecommunications service provider to provide them with identifying subscriber information. This included the

> [n]ame, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address and local service provider identifier that are associated with the subscriber's service and equipment.[18]

At the time, critics were concerned that this effectively amounted to a mandatory identification regime, undermining Internet anonymity.[19] The federal government claimed, controversially, that such mandatory identification was required to fight crimes such as child pornography.[20] After a great deal of public controversy over the warrantless access regime, Bill C-30 was shelved.

However, now that we have learned more details regarding some of the ways in which CSE and the NSA have built tracking tools, we can see how mandatory warrantless access to some forms of subscriber data could also enable the tracking of individuals. Bill C-30 did not place any kind of constraint on requiring access to this information, except in relation to who could require it.[21] It is true that Bill C-30 would not have allowed CSE to ask for subscriber information. However, part of CSE's mandate is to provide technical assistance to other Canadian authorities, including CSIS and the RCMP, who could get access to this data and who would face no legal impediment to setting up a regime of bulk access to this data.

As computer security expert Bruce Schneier writes, "If the NSA has a database of IP addresses and locations, it can use that to locate

users."[22] We know from the recent CSE disclosures that the ability to track individuals in real time through the use of various forms of metadata, including IP addresses, was known to the government at least as early as May 2012.[23] Bill C-30 received first reading in February 2012 and was shelved amidst public protest in February 2013.[24] Therefore, it is perfectly conceivable that the federal government knew that Bill C-30 could enable the deployment, by either CSIS or the RCMP, with the assistance of CSE, of the kind of real-time tracking tools recently revealed. However, such capabilities were not part of the federal government's public discussion of Bill C-30.

In November 2013, the federal government reintroduced lawful access reform as part of its cyberbullying legislation, and in December 2014 these reforms became law.[25] The new lawful access provisions do not include mandatory warrantless access to subscriber information. However, this did not mean that the issue disappeared. Rather, it shifted to the courts in relation to the question of voluntary, rather than mandatory, warrantless access to subscriber information.[26] A number of lower court decisions suggested that it is permissible for the state to get warrantless access to some forms of subscriber information where this information is voluntarily provided by the service provider and where that service provider has a service agreement with its customer indicating that it might share this information with the state.[27] Although many were concerned that legally permissible warrantless access to subscriber information was facilitating large-scale data collection by the state, it is important to note that the legal cases were being argued within a very specific and narrow context — a specific criminal investigation into child pornography — where these broader implications for how such cases might be interpreted to enable very different forms of surveillance were not at all part of the public discussion. In June 2014 the Supreme Court of Canada weighed in and decided, in *R v. Spencer*, that anonymity is an aspect of informational privacy protected by the *Charter of Rights and Freedoms* and that the police require a warrant to obtain subscriber information, even when telecommunication providers are willing to voluntarily provide it.[28] While *Spencer* shuts down many forms of warrantless access, its scope is unclear. For example, the decision emphasized that the police were trying to link a specific person to specific online activities that were being monitored and it is unclear what kind of protections would extend to "bulky" surveillance contexts where lots of data is collected but

remains anonymous (the haystack) in order to help track or locate others (the needle).

Just as the warrantless access issue moved from one of mandatory access to one of voluntary access, the new lawful access provisions make the terms of voluntary access easier. Where a person voluntarily shares information with authorities, so long as she "is not prohibited by law from disclosing" the information, no order is required and there is no criminal or civil liability for providing this information.[29] The Canadian government has suggested that this simply provides "greater certainty" to what is already the case, without providing information as to the contexts in which it seeks voluntary access.[30] It is matched by proposals to amend the federal government's private sector data protection legislation in order to make it easier for organizations to share information with the state, also with virtually no public discussion regarding how this might enable forms of state surveillance.[31]

At a 2014 conference on surveillance, former chief of CSE, John Forster, in response to a question from the audience, indicated that CSE could access its metadata database for the purposes of carrying out its assistance mandate, but that it would then be constrained by whatever legal requirements applied to the institution it was providing assistance to.[32] In other words, if CSE was assisting the RCMP, then its assistance would be governed by the terms of the RCMP's warrant. For those concerned about the domestic implications of broad state surveillance capabilities, this means that the warrant requirements need to be scrutinized with this assistance in mind. Seen in this light, some of the new lawful access reforms are important. For example, there are new production orders for "transmission data" as well as "tracking data" on a standard of reasonable suspicion.[33] The government's rationale is that this is analogous to what we already permit in relation to the use of tracking devices and number recorders.[34] The thought is that since a reasonable suspicion standard was enough when we had to install devices on telephone landlines to determine the numbers phoned, it is enough now to unlock the metadata associated with modern communications. However, we cannot arrive at public understanding of these provisions unless we understand the full context of their use.

What the Snowden revelations have shown us so clearly is that the issue is not about types of information, but *systems* of information and *methods* of analysis. Creating a system of orders and warrants

that presumes meaningful distinctions between subscriber information, transmission data, and content is one that cannot provide the public with a clear understanding of what authorities can actually do and what the privacy implications are. The challenge here is quite serious, as it is not clear that our current constitutional jurisprudence provides us with appropriate legal tools. Our constitutional privacy jurisprudence focuses on types of information, and specifically whether the information meets the "biographical core" test for identifying a reasonable expectation of privacy. What we need are methods of oversight that help us focus on systems and methods.

Jurisdiction and Borderless Communications

When we consider questions of accountability and oversight, we most often do so within a national framework. Canadian commentators, for example, point to systems of oversight south of the border and argue that in comparison our own framework is inadequate and in need of reform.[35] The framing of the question is then how to ensure that Canadian surveillance activities occur within a framework of law, or that Canadians and persons within Canada receive the protection of the law. However, I argue that it is also important to question the extent to which national jurisdiction remains a meaningful category in relation to questions of oversight. As I outline in this section, in the context of a global communications infrastructure, ideas of national law and status categories (like non-US person) are currently more likely to create the legal "loopholes" that enable broad surveillance than to create forms of accountability and oversight.

Our increasingly borderless system of communication is one that follows the technical imperatives of the nature of information. It is widely agreed that the classic point of departure for information theory is Claude Shannon's 1948 paper "The Mathematical Theory of Communication," which purported to provide a theory that would allow one to measure information and system capacity for storage and transmission of information.[36] As he so strikingly outlines in his introduction, the "semantic aspects" of communication — the meaning of messages — "are irrelevant to the engineering problem." "Information," on this model, is not something that is dependent on the context of disclosure or of receipt. One can see how, despite developments in information theory and practice in the intervening decades, this still captures an important aspect of information and

communications technology (ICT). ICT easily shifts information from one context to another partly because what information *is*, is seen to be independent of these contexts. This logic is further extended in the context of the so-called digital revolution in ICT, which has largely erased the differences between different mediums of transmission and led to an ever-greater proliferation of networking.

The basic "logic" of information, therefore, is that it does not respect context. This is one of the reasons that ICT raises so many privacy concerns. Both privacy norms and justifications for the breach of privacy norms depend upon many contextual factors, yet ICT facilitates practices that render those contextual factors irrelevant.[37] Disclosing information in a context and for a purpose different than the context and purpose for which it was initially collected is one example; taking information that is relatively innocuous in one context and aggregating it to create revealing profiles is another. Geographical borders are another "contextual" feature that ICT increasingly renders irrelevant in many practical details. With so many of our personal and professional activities mediated by the Internet, many of us physically sit in one jurisdiction and at the same time talk, shop, write, and read in an entirely different jurisdiction. The rapid adoption of cloud computing has meant that we can now be in one jurisdiction, but have what are essentially our own personal digital archives stored in another jurisdiction (or multiple jurisdictions).

Several NSA surveillance programs exploit these features of modern communications technology through leveraging the fact that much of the world's Internet traffic passes through the United States and that many of the most central players in cloud computing are US companies, giving it a "home-field advantage."[38] Although the NSA's Internet surveillance programs operated extra-legally in the aftermath of 9/11,[39] they now operate within a legal infrastructure that allows them to take advantage of US dominance of the Internet. Prior to 2008, US authorities could only conduct surveillance on non-US person targets outside of the United States by showing reasonable and probable grounds that the target was a foreign power or an agent of a foreign power, and by obtaining an order from the Foreign Intelligence Surveillance Court (FISC).[40] With the passage of the *FISA Amendments Act* (FAA) in 2008,[41] FISC can approve surveillance of non-US persons outside of the United States without individualized orders.[42] These changes have provided the legal basis for NSA

programs like PRISM, which involve obtaining communications data from Internet companies such as Microsoft and Google.

From an American perspective, these legal changes remove obstacles to the timely acquisition of important intelligence information while not compromising US constitutional guarantees, since the US constitution is widely held to not apply to non-US persons abroad.[43] However, from the perspective of a non-US person this can enable state surveillance on standards that fall below their own domestic statutory and constitutional guarantees. Consider Canada. A Canadian using Gmail, for example, has her email routed through the United States and stored on US servers, making it vulnerable to collection under the FAA. Under s. 702, the Attorney General (AG) and the Director of National Intelligence (DNI) are permitted to jointly authorize the targeting of individuals located outside of the United States "to acquire foreign intelligence information."[44] This is not an individualized warrant regime. FISC approves annual certifications for the collection of categories of foreign intelligence information and the AG and DNI can then determine which individuals to target, without any additional oversight.[45] Foreign intelligence information includes information that "relates to…conduct of the foreign affairs of the United States."[46] Such a broad definition can easily include things like political speech, for example; while there are protections in FAA for freedom of expression, these all apply to US persons only.[47] There are also a variety of "minimization" provisions to reduce the privacy impact of authorized surveillance, but these provisions also only apply to US persons.

Canadians do not face a similar threat of surveillance from the Canadian state. For example, the *National Defence Act* does not allow CSE to target Canadians, much less to do so on such lax standard. Canadians can be targeted by CSIS or the RCMP, and then CSE can assist through its assistance mandate, but such targeting is then subject to both the warrant requirements that apply to these agencies as well as our *Charter* guarantees. Of course, CSE has a controversial metadata program that has raised numerous questions regarding both its statutory authorization and its constitutionality. The Snowden revelations have also shown that the CSE is tracking millions of Internet downloads every day, which will inevitably include Canadian Internet activity.[48] Nonetheless, what is important here is that, in relation to non-US persons, FAA permits access to content as well as metadata with fairly limited statutory restrictions

and no constitutional restrictions at all. Canadians who use US-based cloud computing therefore are subject to US state surveillance on standards that, if applied within Canada, would be clear violations of our statutory and constitutional rights.

Many have also claimed that these standards are clear violations of international human rights standards. This debate is ongoing, but the official position of the US government is that the protections of the International Convention on Civil and Political Rights only extend to individuals *both* within its territory and within its jurisdiction.[49] The split that cloud computing makes possible — that an individual would be outside its territory but her information subject to US jurisdiction — also creates a space where international human rights norms (arguably) do not apply.

There has been pressure to amend US law in order to erase this distinction between US and non-US persons. The President's Review Group offered one of the most serious attempts to justify some form of such a distinction. The justification they offer is not based upon the reach of the Fourth Amendment, but an understanding of democratic community. It is worth reproducing at some length:

> To understand the legal distinction between United States persons and non–United States persons, it is important to recognize that the special protections that FISA affords United States persons grew directly out of a distinct and troubling era in American history. In that era, the United States government improperly and sometimes unlawfully targeted American citizens for surveillance in a pervasive and dangerous effort to manipulate domestic political activity in a manner that threatened to undermine the core processes of American democracy. As we have seen, that concern was the driving force behind the enactment of FISA.
>
> Against that background, FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also — and fundamentally — a deep concern about potential government abuse within our own political system. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact

> special restrictions on government surveillance of those persons who participate directly in its own system of self-governance.[50]

The justification for the distinction therefore remains rooted in ideas of the importance of national jurisdiction and traditional ideas of the significance of the state and its coercive powers. This just underscores the fundamental tension: we have a global communications network where increasingly borders do not matter, we have surveillance practices responding to this reality, and yet we seek to justify and hold surveillance powers to account through asserting that borders matter. Even the idea that concerns about abuse of state authority are restricted to the context of domestic political activity is difficult to accept when so many of us frequently cross borders for both personal and professional reasons. The Canadian example of Maher Arar is a stark reminder of this: Arar was apprehended by US authorities while in transit in New York and removed to Syria, where he was tortured.[51]

Apart from the issue of Canadians crossing the border and becoming directly subject to US jurisdiction, there is the issue of information sharing between the United States and Canada, as well as with other allies. If US authorities can collect information about Canadians on lower standards than are permitted within Canada, and then share this information with Canadian authorities, then this effectively creates an end-run around our constitutional guarantees even if it is, on some level, "lawful." Although we do not know enough about Canadian practices to assess the seriousness of this worry, recent evidence suggests it is not that far-fetched.

In a controversial 2014 Federal Court decision, many important details came to light regarding the Canadian government's understanding of information sharing practices between its allies.[52] The case concerned whether when obtaining a warrant from the Federal Court, CSIS needed to disclose the fact that it would seek assistance from CSE under CSE's assistance mandate, and that CSE would task foreign allies with this assistance. Justice Mosley's concern was not with the flow of information from foreign allies to Canadian authorities, but the other way around — that asking for assistance means that the targets of surveillance could face an increased risk of detention or harm from those foreign allies.[53] The issues are legally complex, and the case is being appealed to the Supreme Court of Canada. Here, I merely want to underscore a number of important details that bear

on the question of whether Canadian authorities can obtain information about Canadians that was collected under foreign domestic laws that violate our own constitutional standards.

Partly at issue was a 2007 Federal Court decision that held that the Federal Court did not have the jurisdiction to issue a warrant for surveillance activities abroad.[54] CSIS argued that, in light of this decision,

> they turned to the general authority to investigate threats to the security of Canada set out in s.12 of the [CSIS] Act. They reached the conclusion, through the advice of their legal counsel, that a warrant was not required for CSIS to engage the assistance of the second parties through CSEC [CSE] to intercept the private communications of Canadians outside the country.[55]

It was also CSE's position that no warrant was required for this foreign assistance, that only domestic law of the foreign nation would apply.[56] Accordingly, "they could request that a foreign agency do within its jurisdiction that which CSIS and CSEC could not do in Canada without a warrant."[57] Consistent with this, the Deputy Attorney General of Canada has taken the position that CSIS can ask CSE to task foreign allies to conduct surveillance abroad so long as such surveillance is in accord with the foreign ally's domestic legislation and does not raise serious human rights concerns.[58]

This view partly rests on cases like *R v. Hape*, which have held that when Canadian authorities conduct surveillance on Canadians in other countries the *Charter* does not apply.[59] However, there remains uncertainty as to whether Canadian authorities require some form of lawful authority to conduct surveillance abroad, including engaging the assistance of its allies, even if the *Charter* does not apply.[60] Indeed, the federal government has introduced reforms that would allow CSIS to obtain a warrant with extraterritorial effect.[61] There are also questions as to whether the broad powers legally argued for have actually been exercised.[62] Nonetheless, it shows that there is a plausible legal interpretation that suggests the following asymmetry: there are circumstances where Canadian authorities can ask US authorities to intercept the communications of Canadians on standards that fall far below the level of rights protection afforded to Canadians under our own domestic legislation and constitutional

guarantees. In doing so, they would not be acting unlawfully, given the interpretation of the law just outlined.

What these various examples underscore is that we cannot simply focus on domestic institutions and domestic laws if we are to bring surveillance practices within an effective regime of oversight and accountability. Some form of international treaty is likely required with international oversight bodies. Early in the lifecycle of the Snowden revelations there was speculation about the existence of "no spy" agreements between members of the Five Eyes alliance,[63] protecting the citizens of each country from spying from other members. Although there seem to be informal practices and conventions, the United States has publicly and emphatically denied any formal agreements.[64] Whatever we might think about these relationships "based on decades of familiarity, transparency, and past performance between the relevant policy and intelligence communities," these are not legal protections.[65] They are secret, of uncertain scope, can be discarded in the interests of national sovereignty,[66] exist to protect the interests of the state and not the citizens of that state, and are in no way subject to independent oversight.

Conclusion

It is clear that Canada needs to provide a better system of accountability and oversight for our national security agencies and activities. However, in doing so we need to stop thinking that the issue is illegal activity on the part of our national security agencies, such that the answer is to create a system where we can ensure that they follow the law. Instead, I have argued that we need to start from the proposition that our national security agencies do, in good faith, understand themselves to be acting within the law. If we do that, then we can start to appreciate that the relationship between the surveillance state and the rule of law is much more complex, and the possibility of reform more challenging, than is sometimes clear from reactions to the Snowden disclosures. If we look closely, we will see that surveillance does indeed operate according to a legal infrastructure. The problem is that that infrastructure is one of lawful illegality.

Acknowledgements

I would like to thank David Dyzenhaus and Kent Roach for comments on portions of an earlier draft. I would also like to thank Kent Roach and Hamish Stewart for ongoing discussions regarding the Snowden revelations. All errors are, of course, mine.

Notes

1. For a good discussion of extraterritorial intelligence gathering, see Craig Forcese, "Spies without Borders: International Law and Intelligence Collection," (2011) 5 *Journal of National Security Law & Policy* 179.
2. This was very clear from the remarks of Stephen Rigby, national security advisor to the prime minister and PCO, Michel Coulombe, director of CSIS, and John Forster, chief of CSE, at the hearing of the Senate Committee on National Security and Defence, 3 February 2014. See *Proceedings of the Standing Senate Committee on National Security and Defence*, <http://www.parl.gc.ca/Content/SEN/Committee/412/secd/02ev-51162-e.htm?Language=E&Parl=41&Ses=2&comm_id=76>.
3. Lawrence Hurley, "Supreme Court Will Likely Rule on NSA Programs, Antonin Scalia and Ruth Bader Ginsburg Suggest," Reuters, 17 April 2014, <http://www.huffingtonpost.com/2014/04/17/supreme-court-nsa_n_5170559.html>.
4. David Dyzenhaus, *The Constitution of Law: Legality in a Time of Emergency* (Cambridge: Cambridge University Press, 2006) at 3.
5. *Ibid.* See also Adrian Vermuele, "Our Schmittian Administrative Law," (2009) 122:4 *Harvard Law Review* 1095; Evan J. Criddle, "Mending Holes in the Rule of (Administrative) Law," (2010) 104:3 *Northwestern University Law Review* 1271.
6. President Barak Obama, Address (Speech delivered at the National Defense University, 23 May 2013), The White House, <http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>.
7. John Ashcroft, *Never Again: Securing America and Restoring Justice* (New York: Center Street, 2006); Juliette Kayyem, "Never Say 'Never Again': Our Foolish Obsession with Stopping the Next Attack," *Foreign Policy*, 11 September 2013, <http://foreignpolicy.com/2012/09/11/never-say-never-again/>.
8. As Roach has argued, this debate is not about emergencies per se so much as the rights of terrorist suspects. See Kent Roach, "Ordinary Laws for Emergencies and Democratic Derogations from Rights," in *Emergencies and the Limits of Legality*, ed. Victor V. Ramraj (Cambridge: Cambridge University Press, 2012) at 229.

9. Greg Weston, Glenn Greenwald & Ryan Gallagher, "CSEC Used Airport Wi-Fi to Track Travellers: Edward Snowden Documents," *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>.
10. See, for example, the remarks of John Forster, chief of CSE, *supra* note 2.
11. Canada, Office of the Communications Security Establishment Commissioner, *Annual Report 2005–2006* (Ottawa), <http://www.ocsec-bccst.gc.ca/ann-rpt/archives_e.php>, at 9. This disagreement was not about the metadata program.
12. Canada, Office of the Communications Security Establishment Commissioner, *Annual Report 2006–2007* (Ottawa), <http://www.ocsec-bccst.gc.ca/ann-rpt/2006-2007/cover_e.php>, at 2; Canada, Office of the Communications Security Establishment Commissioner, *Annual Report 2008–2009* (Ottawa), <http://www.ocsec-bccst.gc.ca/ann-rpt/2008-2009/cover_e.php>, at 2; Canada, Office of the Communications Security Establishment Commissioner, *Annual Report 2012–2013* (Ottawa), <http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/cover_e.php>, at 7–8 (Commissioner Décary discussing his disappointment that the government has not made the legislative amendments called for as a response to this dispute. The commissioner also noted that 92 per cent of the commissioners' recommendations since 1997 have been implemented, at 3).
13. David Cole, "Where Liberty Lies: Civil Society and Individual Rights After 9/11," (2011) 57 *Wayne Law Review* 1203 at 1204–5.
14. Federal Court, Edgar Schmidt, and the Attorney-General of Canada, Statement of Claim, Court File No. T-2225-12, *Voices-Voix* <http://www.slaw.ca/wp-content/uploads/2013/01/Edgar_Schmidt_Statement_of_Claim.pdf>, at para. 12, emphasis in original.
15. Lon Fuller argues that a "strong commitment to the principles of legality compels a ruler to answer to himself, not only for his fists, but for his elbows as well." Lon L. Fuller, *The Morality of Law* (New Haven, CT: Yale University Press, 1969) at 159.
16. Edward Snowden, Address (Delivered at the European Parliament, 7 March 2014), <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.
17. This was recently highlighted in the Office of the Privacy Commissioner of Canada, *Special Report to Parliament: Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance*, (Ottawa: 28 January 2014), <https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp>.
18. Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, 1st Sess., 41st Parl., 2011–2012, cl 16.

19. Lisa M. Austin & Andrea Slane, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations," (2011) 57 *Criminal Law Quarterly* 486.
20. Fred Chartrand, "Vic Toews Accuses Bill's Opponents of Siding with Child Pornographers," *Toronto Star* (Toronto), 13 February 2012, <http://www.thestar.com/news/canada/2012/02/13/vic_toews_accuses_bills_opponents_of_siding_with_child_pornographers.html>.
21. Bill C-30, *supra* note 18.
22. Bruce Schneier, "Finding People's Locations based on Their Activities in Cyberspace," *Schneier on Security* (blog), 13 February 2014, <https://www.schneier.com/blog/archives/2014/02/finding_peoples.html>.
23. Communications Security Establishment Canada, *IP Profiling Analytics & Mission Impacts*, 10 May 2012, <http://www.cbc.ca/news2/pdf/airports_redacted.pdf>.
24. Laura Payton, "Government Killing Online Surveillance Bill," *CBC News*, 11 February 2013, <http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384>.
25. Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess., 41st Parl., 2013, cl 20 (first reading 20 November 2013, royal assent 9 December 2014).
26. *R. v. Spencer*, 2014 SCC 43, 375 DLR (4th) 255, 438 Sask R 230, (CanLII).
27. *R. v. Ward*, 2012 ONCA 660, 112 OR (3d) 321, (CanLII). Cases like this suggest that the agreement is just one factor in the reasonable expectation of privacy analysis, rather than a decisive factor.
28. *Supra* note 25.
29. This is the new section 487.0195 of the *Criminal Code*.
30. Government of Canada, Department of Justice, news release, "Myths and Facts Bill C-13, Protecting Canadians from Online Crime Act," November 2013, <http://news.gc.ca/web/article-en.do?nid=832399>.
31. Bill S-4, *An Act to amend the Personal Information and Electronic Documents Act and to make a consequential amendment to another Act*, 2nd Sess. 41st Parl. (first reading 17 June 2014).
32. *The Electronic Surveillance State: Canada's Position, Global Implications & The Question of Reform*, The Canadian International Council, Toronto Branch, 1 March 2014. The question was mine.
33. These are the new sections 487.015, 487.016, and 487.017 of the *Criminal Code*.
34. *Criminal Code*, RSC 1985, c C-46, ss 492.1 (tracking warrant) and 492.2 (number recorder).
35. Weston, Greenwald & Gallagher, *supra* note 9.
36. Claude E. Shannon, "The Mathematical Theory of Communication," (1948) 27 (July) Bell System Technical J 379 and (1948) 27 (October) Bell

System Technical J 623. Reprinted in Claude E. Shannon & Warren Weaver, eds., *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949) at 3.

37. Lisa M. Austin, "Privacy and the Question of Technology," (2003) 22:2 *Law and Philosophy* 119.
38. Glenn Greenwald & Ewen MacAskill, "NSA Prism Program Taps into User Data of Apple, Google and Others," *The Guardian*, 7 June 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
39. James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, 16 December 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>.
40. *Foreign Intelligence Surveillance Act of 1978*, Pub L No 95-511, 92 Stat 1783; US, Senate Committee on Intelligence, 112th Cong, *Report on FAA Sunsets Extension Act of 2012* (S Doc No 112-174) (Washington, DC: US Government Printing Office, 2012) at 16. A "United States person" includes US citizens, permanent residents, unincorporated associations that include a substantial number of US citizens and permanent residents, and corporations incorporated in the United States. See 50 USC § 1801 (i).
41. *FISA Amendments Act of 2008*, Pub L No 110-261, 122 Stat 2463.
42. *Report on FAA Sunsets Extension Act*, *supra* note 40 at 3. At the same time, the FAA increased the protections provided to US persons located outside of the United States, primarily through providing for judicial review.
43. *Ibid.* at 16.
44. *Supra* note 39.
45. President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," *The White House* (blog), 18 December 2013, <http://www.whitehouse.gov/blog/2013/12/18/liberty-and-security-changing-world>, at 135, emphasis in original.
46. See 50 USC § 1801 (e).
47. The President's Review Group reports that section 702 is only used to intercept communications where the foreign intelligence information at issue is "related to such matters as international terrorism, nuclear proliferation, or hostile cyber activities" (*supra* note 43 at 152–3). However, the language of section 702 and the definition of foreign intelligence information does not contain any such limitations.
48. Amber Hildebrandt, Michael Pereira, & Dave Seglins, "CSE Tracks Millions of Downloads Daily: Snowden Documents," *CBC News*, 27 January 2015, <http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120>.

49. Charlie Savage, "U.S., Rebuffing U.N., Maintains Stance That Rights Treaty Does Not Apply Abroad," *New York Times*, 13 March 2014, <http://www.nytimes.com/2014/03/14/world/us-affirms-stance-that-rights-treaty-doesnt-apply-abroad.html?_r=0>.
50. President's Review Group, *supra* note 43 at 153–4, emphasis in original.
51. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar* (Ottawa: 2006), <http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/26.htm>.
52. *X (Re)*, 2013 FC 1275, [2010] 1 FCR 460, 369 DLR (4th) 157, (CanLII), affirmed 2014 FCA 249.
53. *Ibid*. at paras. 115, 122.
54. Reasons for Order and Order (22 October 2007), Justice Blanchard. The public redacted version is *Canadian Security Intelligence Service Act (Re)*, 2008 FC 301, [2008] 4 FCR 230, 356 FTR 56, (CanLII).
55. *X (Re)*, *supra* note 49 at para. 94.
56. *Ibid*. at para. 58.
57. *Ibid*. at para. 60.
58. *Ibid*. at para. 34.
59. *Ibid*. at para. 29; *R. v. Hape*, 2007 SCC 26, [2007] 2 SCR 292, 280 DLR (4th) 385, (CanLII).
60. *X (Re)*, *supra* note 49 at para. 30.
61. See section 8 of Bill C-44 *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, 2nd Sess. 41st Parl.
62. *Ibid*. at para. 112. "I am satisfied that the Service and CSEC chose to act upon the new broad and untested interpretation of the scope of s 12 only where there was a 30-08 warrant in place." The original 30-08 warrants under discussion were issued for surveillance within Canada on targets who were then travelling abroad, so additional warrants were then sought (at para. 36).
63. The members are the United States, Canada, the United Kingdom, Australia, and New Zealand.
64. The President's Review Group, *supra* note 43 at 175; Jennifer Epstein, "U.S. Doesn't Have 'No-Spy' Agreement with Foreign Countries, Obama Says," *Politico*, 11 February 2014, <http://www.politico.com/story/2014/02/nsa-spying-foreign-countries-103382.html>.
65. The President's Review Group, *ibid*. at 175.
66. *X (Re)*, *supra* note 49 at para. 17.

Page left blank intentionally