Introduction

Edward Snowden burst into the public consciousness in June 2013 with a series of astonishing revelations about US surveillance activities. The Snowden leaks, which have continued for more than eighteen months, have confirmed that fears of all-encompassing network surveillance and data capture that were envisioned as worst-case scenarios more than a decade ago have become reality. With scant debate or public awareness, surveillance agencies around the world have become remarkably adept at capturing network communications at the very time that billions of people have come to rely on the Internet as their primary tool for communication, social connection, and information gathering. As a result, the "open Internet" is a far cry from what millions of users might have otherwise expected or believed, with openness more aptly referencing their openly accessible private communications.

Snowden's primary focus has been centred on the United States. However, the steady stream of documents have laid bare the notable role of allied surveillance agencies, including the Communications Security Establishment (CSE), Canada's signals intelligence agency. The Canadian-related leaks — including disclosures regarding surveillance over millions of Internet downloads, airport wireless networks, spying on the Brazilian government, and the facilitation of spying at the G8 and G20 meetings hosted in Toronto in 2010 — have

unsurprisingly inspired some domestic discussion and increased media coverage of privacy and surveillance issues.

Yet, despite increased public and media attention, the Snowden leaks have thus far failed to generate sustained political debate in Canada. Privacy issues, particularly lawful access and warrantless disclosure of Internet and telecom subscriber information, emerged as important issues in 2014 and forced the government to respond to mounting concerns over the privacy protections afforded to Canadians' personal information. Moreover, the Supreme Court of Canada issued the landmark *R. v. Spencer* decision in June 2014, which removed any lingering doubt that Canadians have a reasonable expectation of privacy in subscriber information.

While that decision may have led to changes in law enforcement practices, and revelations about subscriber information requests resulted in some uncomfortable questions in the House of Commons, neither had any discernable impact on the broader legislative agenda. Bill C-13, the government's lawful access bill, received royal assent months after the *Spencer* decision, with no significant amendments or reforms incorporated into the bill in response to the decision. In fact, the shocking attack on Parliament Hill in the fall of 2014, in which a single gunman killed a Canadian soldier and then penetrated deep into the Parliament buildings, only stiffened government resolve for increased surveillance and police powers. By January 2015, the government moved swiftly to introduce Bill C-51, the anti-terrorism bill, which greatly expands information sharing between CSE, the Canadian Security Intelligence Service (CSIS), and fifteen other government departments and agencies.[1]

Notwithstanding the somewhat muted initial political response to the Snowden leaks in Canada, the issue of privacy and surveillance seems certain to remain very much in the public eye. As politicians, policy makers, and the broader public grapple with the long-term implications of surveillance activities, this book aims to enhance the public debate by providing a Canadian perspective on the legal issues.

The nine contributions in the book are grouped into three parts: understanding surveillance in Canada, legal issues, and prospects for reform and accountability. Each contribution is briefly introduced below, but two themes run throughout the book.

The first theme is secrecy. That secrecy is linked to surveillance may seem unsurprising. However, secrecy now extends far

beyond the specific surveillance programs or activities undertaken by Canada's surveillance agencies. For example, Canada's network architecture remains largely shrouded in secrecy, with the lack of domestic Internet exchange points creating a network framework that diverts considerable domestic traffic through the United States. Moreover, Canada's legal framework is often hidden behind ministerial authorizations that are not public, judicial decisions that are secret or heavily redacted, and government legal opinions that are privileged and confidential.

The second theme points to serious cracks in the Canadian surveillance law framework. Contributors point to a myriad of problems with a legal framework that appears ill-equipped to address modern-day communications networks and privacy expectations. Several contributors raise concerns related to global networks, cross-border information sharing, the legal treatment of metadata, and the efficacy of current oversight mechanisms. As the fault lines become larger, a robust public and political debate is needed. While there is no shortage of potential changes — most authors offer their own recommendations — successfully transitioning toward a reform agenda represents an enormous challenge for all concerned with privacy and surveillance in Canada.

I am honoured to have served as editor (and to have contributed my own work on why oversight alone will not address the privacy problems associated with Canadian surveillance), but it should be noted that contributors were granted total freedom to address any aspect of the issue as they saw fit. There was no editorial attempt to prescribe a particular outcome or perspective. Indeed, the contributors differ in their views of Canadian surveillance and the need (if any) for reform. Moreover, while the contributions fit neatly within three sections, each contribution stands on its own and can be read independent of the others.

Part I: Understanding Surveillance

The book opens with two contributions that help unpack the realities of modern Canadian surveillance technologies and programs. Andrew Clement and Jonathan Obar place the spotlight on Canada's Internet infrastructure, coining the term "boomerang routing" to call attention to the fact that a significant portion of Canadian Internet traffic transits through the United States, even when the sender and

recipient are both located within Canada. The surveillance implication of boomerang routing is that Canadian data is more easily accessed by US surveillance agencies.

For example, an examination of thousands of data routes originating in Canada revealed that nearly one-quarter transited through the United States on their way to Canadian destinations. In every instance, the US transit point was a city with a known National Security Agency splitter that would allow for potential capture of the Canadian transmission. In fact, Clement and Obar note that accessing Canadian government websites, as well as major banks and other financial institutions, often involves an exchange in the United States.

The Clement and Obar contribution persuasively argues that the boomerang routing effect has major implications for privacy and network sovereignty. The authors suggest that the solution does not lie in legal reforms, but rather in the creation of a Canadian network architecture that is more likely to retain domestic Internet traffic within the country. They note that this will require the development of new Canadian Internet exchange points, which will decrease the costs of network exchange and make Canadian-based exchanges more likely.

While Clement and Obar reveal the intricacies of Canada's Internet infrastructure and its implications for network surveillance, Steve Hewitt focuses on the limits of network-based surveillance by discussing the role of covert human intelligence sources in Canada. Hewitt starts by arguing that surveillance does not affect all people equally. Rather, "certain groups and individuals have long been subjected to more intrusive surveillance and dramatic consequences because of their ideology or race and ethnicity, or gender or sexuality or religion or nationality or some combination of these factors."

Hewitt notes that technology is often involved in increased intrusive targeted surveillance, yet it would be a mistake to overlook the role that human intelligence continues to play in such activities. Hewitt's concern stems from the likelihood that this form of surveillance will be largely overlooked as politicians and the public grapple with the post-Snowden environment and the urge to focus attention on network-based surveillance.

Hewitt's contribution offers an intriguing look back at the role of human intelligence sources in Canada, which dates to the very founding of the country. Even as technological surveillance emerged as an increasingly important source of information, there remained a

critical role for human intelligence sources. For example, Hewitt notes the limitations of the effectiveness of technological surveillance, as e-mails may be encrypted or coded messages used within network communications. Indeed, he points to a 1996 US congressional report that explicitly addressed the limitations of such surveillance:

> They [technological surveillance] do not, however, provide sufficient access to targets such as terrorists or drug dealers who undertake their activities in secret or to the plans and intentions of foreign governments that are deliberately concealed from the outside world. Recruiting human sources — as difficult, imperfect, and risky as it is — often provides the only means of such access.[2]

While technology has evolved since 1996, Hewitt's contribution emphasizes the need for a more holistic perspective on surveillance that broadly incorporates reforms such as warrant-based oversight.

Part II: Legal Issues

Three contributors provide a legal lens on the Canadian privacy and surveillance issues in a post-Snowden environment. Tamir Israel's contribution focuses on the foreign intelligence issues raised by a networked environment that necessarily cuts across national borders. Israel provides helpful context behind the legal frameworks that support signals intelligence activities, noting that the mandates extend far beyond imminent and serious threats. Moreover, the current frameworks offer limited oversight, with most legal interpretations remaining secret.

Israel is critical of the broad powers granted to CSE, maintaining that the agency is rarely forced to justify its decisions before the courts. The scope of its powers juxtaposed with the lack of public review is stunning: few judicial decisions, legally privileged Department of Justice opinions, and ministerial authorizations that only see the light of day in response to access to information requests. Given the secrecy, Israel argues that assessing CSE's conduct is exceptionally challenging.

Israel also links the legal challenges with CSE's relationship with foreign intelligence agencies, most notably the "Five Eyes" consortium of Canada, the United States, the United Kingdom, Australia,

and New Zealand. He notes that "while CSE cannot obligate its Five Eyes partners to adopt *Charter*-compliant information gathering activities, it *can* more effectively constrain its own intelligence gathering and tasking of FVEY [Five Eyes] resources to reflect the privacy of affected targets."

Lisa Austin's contribution builds on this analysis by focusing on what she describes as "lawful illegality." Her key insight is that discussion of the legality of surveillance requires a careful analysis of the systemic features of surveillance that place a strain on the rule of law.

Austin provides three examples of how the legal surveillance framework itself raises serious concerns. First, she identifies the emphasis on secrecy, particularly in a national security context. Echoing Israel's concern with the lack of transparency associated with CSE review, Austin notes that the secrecy of the legal framework invariably leads to unilateral, rather than objective (and public), interpretations of the law.

Austin also points to the legal concerns that arise through the blurring of law enforcement, border control, and terrorism investigations. By creating legal reforms that apply in all contexts, it becomes exceptionally difficult for the participants in the reform process to effectively account for the implications of legislative proposals or court decisions. The obvious example in this regard is the Canadian government's lawful access legislation, which is also the focus of Christopher Parsons's contribution in Part III.

While the complexity of domestic reforms hampers the legislative process, Austin also cites the international challenge posed by surveillance activity that effortlessly cuts across national borders. Her work builds on the Clement and Obar contribution by layering the legal implications on top of the cross-border network architecture that is the focal point of their analysis.

If Austin's legal analysis raises troubling questions about the broader implications of the legal surveillance framework, Craig Forcese narrows the discussion by highlighting the issues arising from CSE's metadata program. Previously confined largely to technical experts, the Snowden revelations brought the collection and use of metadata into the popular lexicon. The US metadata program has attracted the lion's share of debate, yet Forcese expertly chronicles how Canada has also long maintained a metadata collection program that raises similar legal concerns.

Forcese's contribution helpfully describes the growth of CSE's metadata program, drawing on documents obtained under the *Access to Information Act* by *Globe and Mail* journalist Colin Freeze. Forcese explores the program with a comprehensive legal review that draws on statutory definitions, case law, and government documents.

His analysis makes it clear that there remains considerable legal uncertainty regarding metadata collection, both with respect to the CSE's governing statute and under the *Charter of Rights and Freedoms*. He concludes that changes to current practices are needed, including increased use of ministerial authorizations and legislative reform that provides judges with an oversight role over those authorizations.

Part III: Reforms and Accountability

Having assessed the surveillance framework and the resulting legal issues that arise in Canada, Part III turns to potential reforms and developing more effective accountability mechanisms.

Kent Roach's contribution points to gaps in accountability for surveillance activities and discusses several potential remedies. Drawing on his experience with the Arar and Air India Commissions, he notes, "accountability is impossible to achieve if the information is kept secret from those demanding accountability."

Roach also highlights the shortcomings associated with legislative and judicial accountability. In the aftermath of the Snowden leaks, many commentators (including members of Parliament) have emphasized the benefits of strengthened parliamentary review. Yet Roach cautions that parliamentary reviews are often hamstrung by limited access to secret information, while specialized courts run the risk of being seen as too close to the government. As a result, those reviews may do little to enhance public confidence.

While Roach does not reject parliamentary and judicial accountability mechanisms, he argues that the most effective mechanism lies with the executive. In Canada, these mechanisms include the role of retired judges as commissioners for the CSE who are granted substantial public inquiry powers. Moreover, Roach cites the benefits of whistle-blowing, which, though controversial, has repeatedly succeeded in placing surveillance issues on the public agenda.

Reg Whitaker provides an alternate perspective on accountability, drawing on the importance of Snowden and other whistleblowers to make the case that their work is better understood as

"guerilla accountability" that arises in the absence of official forms of accountability.

Whitaker emphasizes that the international dimension of the surveillance activities hamstrings domestic review efforts, which are typically limited in scope. The inability to effectively assess activities that involve multiple agencies in numerous countries renders guerilla accountability increasingly important. Indeed, he concludes with a statement that will strike some as obvious and others as controversial:

> unless [there are] truly radical revisions in how official accountability is allowed to operate, most importantly including the expansion of its scope to the international dimension, it is certain that if the powerful spy agencies are to be held to account and to operate under the rule of law, guerilla accountability will remain a necessary part of the process.

My own contribution argues that while the instinctive response to the Snowden leaks may be to focus on improved oversight and accountability mechanisms, the bigger challenge will be to address the substantive shortcomings of the current Canadian legal framework. Indeed, improved oversight without addressing the limitations within current law threatens to leave many of the core problems in place. In short, watching the watchers is not enough.

Some of the areas of concern with the legal framework are canvassed in detail in other chapters: the legal implications of metadata (Forcese), the jurisdictional blurring of surveillance activities (Austin), and the routing of domestic data through the United States (Clement and Obar). My contribution discusses those issues and identifies several additional concerns, including the weakness of the Canadian privacy law framework, the lack of legal protection found in cross-border data transfer agreements, and the limited protections afforded to Canadians once data is collected by US agencies.

I conclude that as Canadians learn more about the current state of surveillance activities and technologies, there is a budding recognition that current surveillance and privacy laws were crafted for a much different world. The recent call for improved oversight and accountability of Canada's surveillance agencies is both understandable and long overdue. However, the bigger challenge will be to address the substantive shortcomings of the current Canadian legal

framework, as well as the limitations found in foreign frameworks that have a direct impact on the privacy of Canadians.

Christopher Parsons illustrates the enormity of the reform challenge by providing a case study of the legislative battles over lawful access, a closely related issue. The Canadian policy debate over lawful access extended over a decade, with many of the same stakeholders, and security and privacy concerns that arise within the surveillance discussion.

Parsons's contribution traces back to the initial debates over lawful access in 2001, highlighting the "meandering" policy environment that saw the legislation and its justifications repeatedly change over time. Parsons identifies several factors that are crucial in influencing legislative outcomes, including government responsiveness (namely, minority governments), media coverage, and public engagement.

The lawful access experience provides important lessons for the debate over Canadian surveillance that lies ahead. The Snowden revelations have succeeded in placing Canadian participation in global surveillance activities on the public radar screen. As the contributions in this book demonstrate, Canada's active participation raises critical questions about the sovereignty of the Canadian Internet, the adequacy of the surveillance legal framework, and a myriad of possible reforms to address both legal and accountability shortcomings. If the lawful access debate is any indication, addressing these issues will take many years, as Canadians grapple with how best to strike the balance between privacy and security in a post-Snowden environment.

Notes

1. See http://antiterrorlaw.ca/, a website written by Professors Forcese and Roach that provides an exhaustive analysis of the far-reaching implications of Bill C-51.
2. "Preparing for the 21st Century," http://www.gpoaccess.gov/int/report.html, as quoted in Mark D. Villaverde, "Structuring the Prosecutor's Duty to Search the Intelligence Community for Brady Material," *Cornell Law Review* 88: 5 (2003): 1521.

Page left blank intentionally