Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence

Midori Ogasawara

Abstract

This article offers a transnational perspective on Canada's legislative response to globally expanded national security intelligence activities in the War on Terror since 2001. I situate Canada's new legislation against the backdrop of US and Japanese legislative responses and analyze the transition, including Bill C-13 (2014), Bill C-44 (2015), Bill C-51 (2015), and Bill C-59 (2019). I argue that the thrust of this legislative trend has been the active legalization of previously illegal surveillance activities by security intelligence agencies, rather than passive ineffectiveness in restricting state mass surveillance enabled by information and communication technologies. The transition is in synch with a global legislative trend that lowers the legal standards of privacy and personal data protection and weakens checks and balances in democratic governance. As a result, mass surveillance has increasingly undermined and regulated the rule of law, not vice versa.

Keywords: CSIS, CSE, Bill C-51, policy laundering, retroactive immunity, Five Eyes, Snowden

Résumé

Cet article offre une perspective transnationale sur la réponse législative du Canada à l'élargissement à l'échelle mondiale des activités de renseignement pour la sécurité nationale dans la guerre contre le terrorisme depuis 2001. Je situe la nouvelle législation du Canada dans le contexte des réponses législatives américaines et japonaises et j'analyse la transition, notamment avec le projet de loi C-13 (2014), le projet de loi C-44 (2015), le projet de loi C-51 (2015) et le projet de loi C-59 (2019). Je soutiens que l'idée maîtresse de cette évolution législative a été la légalisation active des activités de surveillance, auparavant illégales, par les services de renseignement de sécurité, plutôt qu'une inefficacité passive à restreindre la surveillance de masse de l'État rendue possible par les technologies de l'information et de communication. Cette transition est en phase avec la tendance législative mondiale à réduire les normes juridiques de protection de la vie privée et des données personnelles et à affaiblir les freins et les contrepoids dans la gouvernance

Canadian Journal of Law and Society / Revue Canadienne Droit et Société, 2022, Volume 37, no. 2, pp. 317–338. doi:10.1017/cls.2022.9

démocratique. Par conséquent, la surveillance de masse mine de plus en plus l'État de droit, cette surveillance devient même une force régulatrice de l'État de droit plutôt que l'inverse.

Mots clés : SCRS, CST, projet de loi C-51, blanchiment politique, immunité rétroactive, « Five Eyes », Snowden

Introduction

Electronic surveillance activities by national security intelligence agencies have inherently global characteristics. This was well-established when Edward Snowden, a former contractor for the United States National Security Agency (NSA), exposed the NSA's signals intelligence (SIGINT) activities, documented in an unprecedented volume of classified files. The files evidenced how the infrastructure, operations, purposes and effects of the intelligence enterprise cross borders and have a global reach.

However, public debate on the legality of digital mass surveillance activities has often remained in the context of a single state. During the Snowden revelations in 2013, American media responded most furiously to the NSA's covert "bulk data collection" from US citizens, such as through Verizon's mobile phones, or the PRISM program, which partnered with major internet corporations such as Google, Facebook, Apple, and Microsoft (Greenwald 2014). The shock stems from US intelligence's routine avowals that they had never spied on their own citizens because the Fourth Amendment of the US Constitution protects people from unreasonable search and seizure by the government (Klein 2009). In the single-state legislation, governments normally draw a line between legal and illegal surveillance by distinguishing between who is being watched, citizens or non-citizens. The NSA files exposed that there was no longer such demarcation in the intelligence operations. The public disillusionment was understandable, but important inquiries for the rest of the world were rarely addressed: Is it OK to spy on non-US citizens as threats to the national security? Don't they have fundamental rights to privacy and personal data protection in international society?

In this article, I bring a transnational perspective to debates on the legality of intelligence activities that have expanded globally since 2001 under the Western "War on Terror." The United States-centric single-state view fails to articulate the common interests of global communities and does not question the overall legality of NSA activities outside US borders. This is in part due to the fact that legislative debates about mass surveillance have been structured around the concepts of privacy and personal data protection, both of which have been traditionally defined as rights held by citizens within a single state (Palfrey 2000; Archick 2006; Bennett and Raab 2006). However, the NSA has clearly transgressed the demarcation line between citizens and non-citizens. Furthermore, novel capacities of information and communication technologies (ICTs) have enabled the flow of data beyond national boundaries, creating a global, electronics-based Surveillance Society (Lyon 2007). Transnational perspective is necessary to examine how this global flow of

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

data has influenced legislative changes beyond a single-state regime of privacy and data protection.

In the past two decades, Canada has experienced drastic changes to legislation on intelligence activities. Despite constant public opposition, both Liberal and Conservative governments have created new laws to help Canada's intelligence agencies expand their surveillance activities. The serial legislation has been increasingly legalizing previously illegal mass surveillance activities that target people inside and outside Canada, particularly involving their personal data through digital networks. While the legal support for intelligence agencies by the governments may look obvious, the fact counters both popular and academic discourses, such that law is never able to catch up to the fast pace of technological development and so has no ability to regulate technology, or that mass surveillance is practiced in the legal "gray" zone. Yes, the accelerating speed of digital technologies indeed creates challenges for regulatory practices, and as digital surveillance is an emerging technology, there was not yet regulation to ban it. However, these dominant views neglect the active role of legislation to legalize previously illegal mass surveillance. I argue that Canada's legislation has been predominantly endorsing illegal mass surveillance activities covertly developed by the intelligence agencies, and that this is threatening the rule of law because it suggests that lawmakers lack the agency to stop illegal surveillance against people by the state. How then can democratic society set a limit on the ever-growing surveillance game? The carte blanche further implies that the rule of law is losing the foundation of checks and balances in democratic government, dissolving, rather, into the rule of the powerful and privileged who exert extraordinary technological capacities over the population.

A transnational perspective helps unpack this ongoing threat to the rule of law in Canada, as other nations have also drawn similar legislative trajectories involving digital mass surveillance. In the following, I situate Canada's new legislation against the backdrop of US and Japanese legislative responses over the past two decades as part of the global trend, and analyze the transition, including Bill C-13 (2014), Bill C-44 (2015), Bill C-51 (2015), and Bill C-59 (2019). Why the United States and Japan? The United States has been the global epicentre of today's mass surveillance systems, and Japan has been playing a significant role to expand NSA surveillance across the Pacific, as discussed below. Canada positions itself closer to the United States than Japan within the intelligence alliance, so the commonalities (and differences) in the legislative trend are explored. I previously examined US and Japanese legal techniques to support NSA surveillance, based on interviews with Mr. Snowden and AT&T whistleblower Mr. Mark Klein and an investigation of NSA files (Ogasawara 2017, 2021). Since most digital infrastructures are built by multinational corporations based in the United States and the dominant data flow around the world goes through US facilities (Clement and Obar 2015), discrete domestic surveillance legislation must be contextualized by linking global data flows with the political economy behind the commercial and intelligence systems that operate within it.

From this vantage point, I suggest that the thrust of this legislative trend has been to *actively* legalize the previously illegal surveillance activities of security intelligence agencies, rather than to *passively* be ineffective in restricting state mass

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

surveillance enabled by ICTs, let alone defending constitutional rights of citizens. The transition is in sync with a global legislative trend that lowers the legal standards of privacy and personal data protection and weakens checks and balances in democratic governance. As a result, mass surveillance has increasingly undermined and regulated the rule of law, not vice versa.

I start with a brief overview of the global and collaborative characteristics of mass surveillance, disclosed by the NSA files. The global operation of mass surveillance systems can be best laid out in the infrastructures collaboratively developed by intelligence agencies and technology companies. I then outline how the United States and Japan have developed legal tools to legalize the previously illegal collection of personal data through global communication infrastructures, such as "retroactive immunity" and "policy laundering." Third, I turn to Canada's legislative changes. I divide the era of the War on Terror into three phases and discuss how new bills have accommodated illegal mass surveillance practices in each phase. I explore in the Canadian context similar legal techniques to those used by the United States and Japan. Despite the success of bringing new oversights to intelligence activities in Bill C-59, the whole scale of legislative changes to legalize previously illegal mass surveillance in the past two decades is incomparable with such partial improvement, and this transnational analysis focuses on how the globally intertwined growth of intelligence power threatens the rule of law in each country. This analysis implies that intelligence agencies in all three countries have increasingly developed the ability to shape favourable laws for their own interests to the extent that intelligence agencies stand above constitutional protections, such as the *Canadian Charter of Rights and Freedoms*. Finally, I conclude that, although intelligence agencies have exercised power within a single state to legalize mass surveillance, this cannot overturn international law and the principles of human rights and peace. A transnational perspective is necessary to examine the full scope of the consequences resulting from digital mass surveillance on a global scale.

The Global and Collaborative Characteristics of Mass Surveillance

Scholars often define surveillance as the "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007, 14). Security intelligence agencies also collect personal data for those purposes. But, because they work in the fields of crime control and war, their surveillance activities may result in drastic actions, such as detention of suspects or disruption of potentially criminal acts, beyond just watching over people. The key is that decisions are made based on the personal data they collect.

The global characteristics of electronic mass surveillance can be captured at a glance by one of the NSA's top-secret slides, disclosed by Snowden: International Cables (Figure 1).

Transoceanic cables have long been the main vessels of electronic communications, and fiber-optic cables have been increasingly constructed for ever faster and wider exchange of information in the internet age. New plans for communications infrastructure have constantly been negotiated as a multinational project in different locations of the world, from small islands in the Pacific to East Asian

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

Figure 1 International Cables.

shores, in order to expand the global political economy and colonial outposts (Starosielski 2015). These are the exact sites where the NSA collects global communications, called "Special Source Operations" (SSO) (Greenwald 2014).

The SSO play a central role in today's covert data acquisition. Telecommunications companies from different countries jointly build and operate the cables, and locate the landing stations onshore to sort data traffic. The NSA requires the telecoms to set up a room for the NSA to copy all data going through the landing sites, which are called "choke points" (Greenwald 2014). For example, one of the SSO programs, code-named STORMBREW, has seven choke points on the west and east coasts of the United States, where the transoceanic cables land from the Pacific and Atlantic.

Across the Pacific, STORMBREW operates on the Trans-Pacific Express submarine cable system, which was built in 2008 by US telecoms Verizon and AT&T, Japan's NTT Communications, and five other telecoms in China, Taiwan, and South Korea (Figure 2).

STORMBREW captures incoming information from East Asia. Massive international flows of communication data are not necessarily directed to websites, accounts, or devices in North America, but they technically go through servers or other facilities run by global ICT companies, often based in Silicon Valley. The NSA is aware of this geolocational advantage. As such, the SSO were enabled by big techs and telecoms, like Verizon and AT&T. The Snowden files revealed the "extreme willingness to help" on the part of Verizon in the case of STORMBREW and AT&T in the case of another SSO program, FAIRVIEW (Angwin et al. 2015). Likewise, the

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

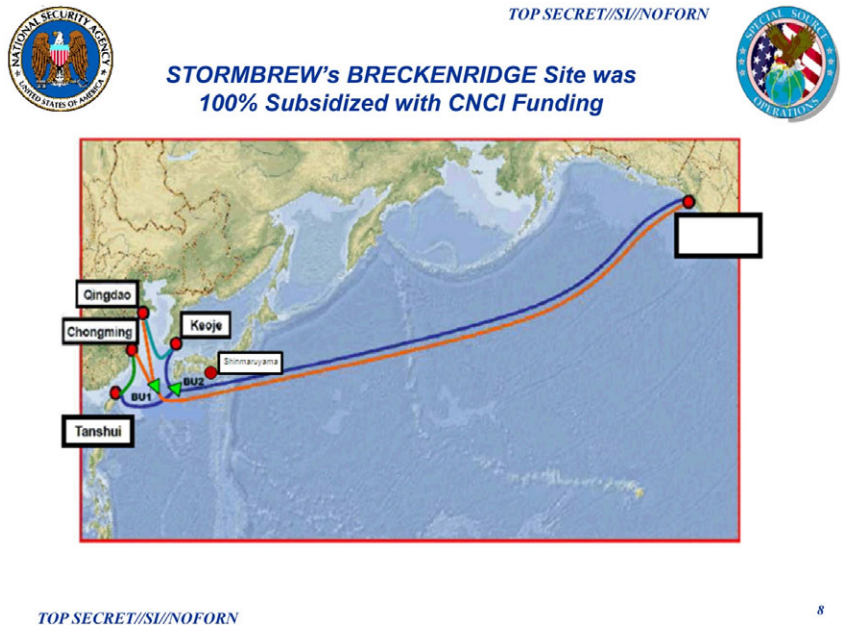

Figure 2 STORMBREW operates on Trans-Pacific Express cables, tying the United States to Shinmaruyama (Japan), Tanshui (Taiwan), Keoje (Korea), and Qingdao and Chongming (China).

PRISM program was created with the collaboration of internet service providers Microsoft, Yahoo!, Google, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple, which provide the NSA with customers' personal data. Mass surveillance has collaborated with private companies to systematically operate worldwide. Data from the internet and other digital communications has been transmitted beyond national borders on commercial and private bases, which has also helped obscure the mass surveillance operations by states.

Today's communications infrastructure characterizes global connections as well as global surveillance networks. The NSA has been copying communication data without people's consent or court warrants with the cooperation of big data corporations. This is illegal in democratic jurisdictions that ban the state from conducting unreasonable search and seizure against its people, whether it is the United States, Japan, or Canada. But has any law enforcement investigated or arrested NSA agents or big tech executives? No. This proves the extrajudicial power of security intelligence agencies. The question then should be asked the other way around: How has the global expansion of illegal intelligence activities changed democratic jurisdiction so as to obscure wrongdoing?

Legal Innovations to Legalize Illegal Mass Surveillance: Retroactive Immunity and Policy Laundering

In the United States, the epicentre of global mass surveillance, systematic warrantless wiretapping began with a secret executive order by President George W. Bush

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

in the aftermath of 9/11, and the subsequent secret interpretation of the *US Patriot Act* by the Department of Justice (see Gellman 2013). When secrecy was removed, a process of legalizing illegal mass surveillance took place. It was in 2006 that a former AT&T employee, Mark Klein, shared documents with the Electronic Frontier Foundation (EFF), proving that the NSA operated illegal wiretapping within the AT&T building in San Francisco (Klein 2009). Klein, a communications technician, accidentally noticed a secret room for the NSA in his workplace and discovered that a device called a "splitter cabinet" in the room was duplicating incoming data for the NSA, most of which was domestic. This could be seen as an urban version of SSO, happening years before the Snowden revelations.

The EFF, an advocacy group for electronic privacy and free expression, sued AT&T on behalf of its customers (*Hepting v AT&T*) for violating privacy law by collaborating with the NSA in an illegal program to intercept citizens' communications (Electronic Frontier Foundation, n.d.). But Congress passed a controversial bill, the *Foreign Intelligence Surveillance Act [FISA] of 1978 Amendments Act of 2008*, which allowed the Attorney General to require the dismissal of lawsuits over a company's participation in a warrantless surveillance program if the government secretly certified to the court that the surveillance did not occur, was legal, or *was authorized by the president.* The new legislation awarded AT&T so-called retroactive immunity, and, as a result, over forty lawsuits against US telecoms and the NSA were dismissed, including *Hepting* (Clement and Obar 2015).

It is not enough to view retroactive immunity simply as an exception to democratic jurisdiction. It literally subverts the rule of law in two ways: First, "retroactive" goes against the criminal legal principle that law becomes effective only after it is enacted, so people are aware of the rules and can understand what kinds of behaviour are legal and illegal. Second, "immunity" gives extraordinary power to certain entities who don't have to follow the rules, which creates lawlessness and inequality in society. Together, retroactivity and immunity endorse illegal activities and give them a lawful appearance. This legal tool is innovative enough to replace the rule of law with the rule of the powerful: in this case, the intelligence agencies and big tech companies. These two powerful groups already enjoyed secret state privilege, under which they committed illegal mass surveillance, which shows they do not deserve the privilege, or at least that the privilege should be seriously reconsidered. But on the contrary, the powerful not only go unpunished but are also legally protected in future activities by the newly institutionalized impunity. In other words, the illegal acts committed by the executive branch of the democratic government not only escaped checks and balances by the legislative and judicial branches, but the legislative helped the executive, and the judiciary followed. In short, the legal innovation of retroactive immunity can be used to subvert, nullify, and disguise the rule of law under a democratic jurisdiction.

On the other side of the Pacific, Japan enacted a series of surveillance laws from 2013 to 2018, which helped shield the NSA's surveillance activities from the public eye and expanded the capacities of data collection by both the NSA and the Japanese government. The right-wing government, led by Prime Minister Shinzo Abe, proposed the *Secrecy Act* in 2013, on which Snowden commented, "This new state secrets law was actually designed by the United States" (Ogasawara 2017, 480).

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

When Snowden worked for the NSA's Japanese headquarters in the U.S. Yokota Airbase in the suburb of Tokyo from 2009 to 2011, he witnessed the negotiations process: the NSA requested that the Japanese government set a legal wall blocking the public from its illegal surveillance activities by secret state legislation. Snowden described that the NSA has a group of roughly 100 lawyers who work for the Office of General Counsel. They partnered with the Foreign Affairs Directory, which researches the legal limitations in different countries to collaborating with the NSA and how to get around legal protections that prevent these countries from spying on their citizens. These legal experts' work includes hiding the NSA's mass surveillance from the public so the NSA can further expand its global surveillance networks. It is highly problematic in terms of Japanese sovereignty for another country to draft such a law, but the NSA has the clear intent of flattening the legal system to support its own interests and make its illegal activities legal, even outside US jurisdiction.

Following the *Secrecy Act*, the Abe administration enacted the highly controversial *Conspiracy Act* in 2017, which criminalizes people who communicate about committing a crime, even if they do not actually commit any criminal act. Japan had established the democratic criminal justice system after the Second World War that states that no one should be charged for a crime before they take action. Thus, the *Conspiracy Act* is more than just a statute, because it undermines the superior principle of democratic criminal justice. Because of its radical potential to give the police new power to monitor private conversations, it had failed to pass the Diet three times since 2003 (Kaido 2017).

To overcome these hurdles, the Japanese government used the *United Nations Convention against Transnational Organized Crime*, adopted by the General Assembly in November 2000. Abe insisted that Japan needed to create conspiracy crimes to combat terrorism and ratify the UN convention, failing which it could not host the Olympic games in 2020. Because Japan has rarely had terror incidents, harmonizing the national legislation to international demand was the only rationale the government could push. However, the *United Nations Convention against Transnational Organized Crime* does not require the creation of conspiracy crimes against terrorism (Kaido 2017; Hiraoka 2018). The convention was adopted to prevent organized crime, such as human trafficking of women and children or smuggling of migrants, not terror. The government's claim was baseless, but it promoted the Conspiracy bill in the name of international harmony and having a safe Olympics in Japan. The political strategy of creating domestic policy through international organizations and their authorities is called "policy laundering" (ACLU 2005; Bennett et al. 2014) and was effectively used in the Japanese context.

Importantly, the NSA first developed the scheme of creating judicial loopholes with a group of Second Parties, informally called the "Five Eyes" countries (United States, Britain, Australia, New Zealand, and Canada), and then exported it to other countries. This legal strategy was apparently accepted because every foreign intelligence agency wants more data. Snowden emphasized that this not only applies to United States–Japan relations, but in general (Ogasawara 2021). The NSA classifies thirty-three countries as "Third Parties" to the "SIGINT Partners," willing to cooperate with the NSA, including France, Germany, Italy, India, Israel, Norway, Saudi Arabia, Thailand, and Turkey (Greenwald 2014). Whichever

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

category a country belongs to, the NSA has been innovating tools to create a favorable legislative landscape for itself on foreign soil.

In summary, in the expansion of electronic intelligence activities since 2001, the law has not been used to regulate, stop, or punish illegal mass surveillance activities by intelligence agencies. Rather, in the United States and Japan, the law has been actively reformed to accommodate the existing illegal activities by developing new tools such as retroactive immunity and policy laundering. Those legislative responses have not only legalized previously illegal surveillance, but also undermined criminal justice principles and democratic jurisdiction, forming an active power to replace the rule of law with the rule of the powerful. The same types of surveillance legislation have been reported in France, Italy, and other Western countries under the War on Terror (Willsher 2015; European Digital Rights 2015). Against this global backdrop, let us turn to what has happened in Canada, one of the Five Eyes countries.

Three Phases to Legalize Illegal Mass Surveillance in Canada

I divide Canada's legislative responses to mass surveillance in the last two decades into three phases. The first phase extends from the signing of the European *Convention on Cybercrime,* in 2001, to the government's repeated, unsuccessful attempts to gain warrantless access to internet subscriber information up until 2012. The next phase began with Bill C-13 (2014), which legalized warrantless data collection for the first time, and Bill C-44 (2015), which shifted the role of the judiciary to help illegal surveillance activities by Canadian intelligence agencies abroad. The third is marked by the most controversial bills, Bill C-51 (2015), which formalized the extrajudicial power of the intelligence agency over *Charter* rights, and Bill C-59 (2019), which expanded the area of active cyber operations.

Before going into the first phase, a brief explanation of the historical development of Canada's intelligence agencies is needed. Currently, there are two main forces in the field of security intelligence, the Communications Security Establishment (CSE) and the Canadian Security Intelligence Services (CSIS), among other agencies that have also actively collected, retained, and used personal data for security purposes, such as the Royal Canadian Mounted Police (RCMP), Public Safety Canada, and Canadian Border Services.

The CSE practices SIGINT activities as a partner of the NSA. Just like the NSA, its activities originated in the Second World War, and it was institutionalized as the Communication Branch of the National Research Council, while staying low-profile for a long time (West 2016). It was finally authorized under the *National Defense Act* of 1985, which assigned it three specific mandates, with a fourth mandate added through Bill C-59. Mandate A speaks for the importance of a global communications infrastructure for spying, as it is to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence." Foreign intelligence refers not only to national security, but also diplomatic, economic, or other areas of spying. Mandate B is for the "protection of electronic information and information infrastructures." And, most importantly, Mandate C is to assist "federal law enforcement and security agencies

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

in the performance of their lawful duties" (also amended by Bill C-59, as explained below), which suggests constant collaboration with CSIS.

For SIGINT, Canada signed an agreement with the United States (CANUSA) in 1948, following the United Kingdom in 1946 (UKUSA). Australia and New Zealand joined the SIGINT in 1956, these countries later forming the Second Parties of Five Eyes (Lyon and Murakami Wood 2021).

While CSE by definition covers the area of foreign intelligence, CSIS conducts security intelligence in the domestic arena, such as espionage, sabotage, and foreign influence activities on politically motivated violence (Rudner 2002). CSIS was created by the *Canadian Security Intelligence Services Act* in 1984, which separated it from the RCMP because of the serial illegal intelligence activities revealed in the 1970s, which were interestingly parallel to the illegal spying against dissidents by the FBI in the United States during the Civil Rights movement and Vietnam War (Bamford 2001). The government inquiry into the RCMP's security services, the McDonald Commission, found that the RCMP employed active forms of disruption and dirty tricks in terror cases instead of prosecution—surveilled members of Parliament, opened mail, made illegal use of income tax information, and spied on universities and unions (Forcese and Roach 2015). By 1977, the security services had 1.3 million entries in its files about 800,000 individuals, including Canadians who had visited the Soviet Union and known homosexuals (ibid., 40). The McDonald Commission concluded that security intelligence should be taken away from the RCMP and that a new civilian intelligence agency should be subject to a precisely defined legislative mandate under ministerial control and reviewed by a special expert committee.

The historical creation of CSIS is an important reminder of the institutional tendency of security intelligence agencies to use illegal means of investigation. The McDonald Commission also warns us that "access to computer technology greatly facilitates the ease with which information and opinions recorded in these files can be retrieved and correlated" (cited in Forcese and Roach 2015, 40).

Phase One: Policy Laundering through the European Convention on Cybercrime in the Aftermath of 9/11

Canada began to pursue new legislation to legalize previously illegal mass surveillance activities when it signed the Council of Europe's *Convention on Cybercrime* in November 2001. The European Convention can be seen as the first international move for surveillance legislation during the War on Terror. Forty-three countries, including non-member states Canada, Japan, South Africa, and the United States, signed the Convention, which requires participating nations to enact legislation that facilitates investigation and prosecution of crimes committed through the internet (Huey and Rosenberg 2004; Archick 2006). In the name of harmonizing national legislation and improving international cooperation, the signatories attempted to grant law enforcement authorities "lawful access" to data traffic, which compels internet service providers and telecoms to assist interception by the state. Similar legislation had been previously proposed in the United States and

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

United Kingdom but had been dropped because of public concerns about privacy (Palfrey 2000).

The Convention provided a policy laundering detour for those governments (ACLU 2005; Bennett et al. 2014). Although the Convention focused on particular crimes, such as fraud, forgery, child pornography, and copyright infringement, it opened up a much larger sphere over time for state policing and intelligence gathering, which had also been pushed in the context of national security. Compliance with the Convention was used to justify legislation that significantly weakened the legal standards of data protection established in each signatory country (Huey and Rosenberg 2004; Bennett and Raab 2006).

In Canada, the process of granting law enforcement lawful access to personal data started with two consultations in 2002 and 2005 under the Liberal government. The government put together opinions on lawful access from different groups, such as law enforcement, telecoms and internet companies, and privacy advocates. Subsequently, Paul Martin's government introduced the *Modernization of Investigative Techniques Act* (MITA) in 2005. The MITA represented the interests of intelligence agencies and law enforcement clearly: obtaining warrantless access to subscribers' information at telecom service providers, and requiring the providers to create new services and products that are interceptable by the government (Parsons 2015). In other words, these services and products direct telecoms to incorporate tapping facilities in their communications infrastructures, just as AT&T did for the NSA. Around the same time that Klein noticed the NSA's massive wiretapping, practiced at the AT&T branch in San Francisco, a similar effort to embed surveillance devices in communications infrastructure was publicly pursued north of the border. But, unlike the United States, when the Canadian government openly expressed its intent to conduct warrantless wiretapping, it faced public opposition, including from the telecoms. The MITA failed to pass the first reading in Parliament. After the Conservative government came into power in 2006, Prime Minister Stephen Harper restarted the process of negotiating with the industry, in consultation with Public Safety Canada.

The Harper government repeatedly introduced lawful access bills along the lines of the MITA, such as Bills C-46 and C-47 in 2009 and Bills C-50, C-51, and C-52 in 2010. Bill C-30 of 2012, whose first short title was the *Lawful Access Act,* which was then changed to *Protecting Children from Internet Predators Act*, required telecoms to include interception technologies in order to obtain a commercial license. While all these bills died on the Order Paper or were withdrawn, the government's persistent attempts clearly showed a strong impetus from intelligence agencies to legalize their warrantless access to people's communications data. Despite failure to convince the public of the need for mass surveillance over a decade, the impetus to do so has never faded, because Canadian intelligence agencies have already collected people's communication data without legal authorization. The public only learned about it after the Snowden revelations in 2013: CSE had secretly deployed a metadata program, including locations, internet protocol address, or time of personal communication. Minister of Defence Bill Graham in the Liberal government first approved the program by signing a secret decree in 2005, and Minister of Defence Peter MacKay in the Conservative

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

government renewed it formally through a ministerial directive in 2011 (Freeze 2013). Metadata shows a much wider and deeper picture of personal lives than subscriber information, disclosing when, where, and with whom the person communicated, and what she or he did on the internet or phone (Clement, Harkness, and Raine 2021). The government needed new legislation to legalize the metadata program, which could give CSE formal immunity, even retroactively.

This phase shows how secrecy plays an important role in launching mass surveillance programs in the Canadian context, as elsewhere. The European *Convention on Cybercrime* enabled the Canadian government to form a bill, but it could not defeat opposition in the public arena. Then, lacking a legislative basis, the government started the covert metadata program through the secret interpretation of law, which was also the case with the NSA surveillance (Gellman 2013).

Phase Two: Resistance from the Courts and the Accountability Question

The impetus to get lawful access to internet subscriber information in the MITA was reintroduced in Bill C-13 in November 2013. The *Protecting Canadians from Online Crime Act*, or *Cyberbullying legislation*, was passed when the public learned of the tragic suicides of two young women who experienced online harassment. Bill C-13 legally authorized telecom service providers voluntarily to provide subscriber information to law enforcement without warrants. It also allowed a judge to order the disclosure of metadata where there are "reasonable grounds to *suspect*" that an offence has been or will be committed, which lowers the threshold of warrants from "reasonable grounds to *believe*" (emphasis added). Normally, law enforcement needs to provide evidence that is strong enough to have a judge "believe" the offence and issue a search warrant. But Bill C-13 adopted "suspect," which only requires evidence that triggers suspicion, to disclose someone's communication data. "Believe" holds a higher standard of safeguard for privacy than "suspect," in this sense. Put differently, the new law treats subscriber information as having low privacy value.

The voluntary disclosure of subscriber information to law enforcement was, however, soon ruled illegal, in *R v Spencer* in June 2014, six months before Bill C-13 came into effect. The police had no warrant but took personal data from an IP address, and the court decided it had violated Mr. Spencer's constitutional rights under Section 8 of the *Canadian Charter of Rights and Freedoms*, which states "Everyone has the right to be secure against unreasonable search or seizure." The court decided that law enforcement required a warrant to obtain subscriber information, even when telecoms are willing to provide it voluntarily.

Spencer can be seen as a healthy reaction of the judiciary to an executive branch that tends to circumvent judicial oversight over abuse of power, such as warrantless wiretapping. Further judicial scepticism was expressed in June 2013, the month of the Snowden revelations. A Federal Court judge, Justice Richard Mosley, found it illegal that the Canadian intelligence agencies tasked foreign agencies to conduct interceptions on Canadians. In 2009 in the Federal Court, Mosley gave permission to CSIS to spy on Canadians abroad but later discovered that CSIS asked CSE to task their foreign partners with this assignment. In fact, CSIS and its lawyers had

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

lied to the court "about their intention to seek the assistance of foreign partners," and this would "involve the breach of international law by the requested second parties" (cited in Whitaker 2015, 215). CSIS strategically omitted disclosing information to exclude any reference to the role of second parties: the deception of the court revealed not only the extrajudicial character of the intelligence agency, but the way information laundering has become routine among the Five Eyes countries. Reg Whitaker calls it the failure of official accountability, because the reviewing bodies of the Security Intelligence Review Committee (SIRC) and the CSE Commissioner had not flagged any possible human rights violations resulting from information laundering. Instead, the judge who carefully read the reports produced by SIRC and the CSE Commissioner noticed illegal surveillance activities. It is the rise of what Whitaker calls "guerilla accountability" (Whitaker 2015, 215), like Snowden's, that will blow the whistle for a democracy in crisis.

Importantly, Mosley's caution about information sharing with foreign agencies reflected the horrible human rights violation cases conducted by the Five Eyes. A well-known case was Canadian citizen Maher Arar's extrajudicial rendition to Syria in 2002. The RCMP provided the FBI and CIA with an investigation on Arar and asked them to place Arar and his wife under surveillance, describing them as "Islamic extremists" associated with Al Qaida, although they were not (Webb 2007; Forcese and Roach 2015). As a result, US officials arrested Mr. Arar in transiting flights in New York and sent him to Syria via Jordan, where he was detained for approximately one year and tortured. After the return of Arar and other citizens to Canada, two public inquiries were formed and found that information sharing between RCMP, CSIS, and foreign agencies resulted in serious physical and mental abuses of innocent citizens, through essentially one-sided and deeply prejudiced racial profiling. The Arar Commission recommended that information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture (Forcese and Roach 2015).

Justice Mosley's action and the *Spencer* decision were desirable interventions by the Canadian judiciary into the growing mass surveillance networks of intelligence agencies and law enforcement. In both cases, the judiciary directed agencies to refrain from illegal surveillance activities and maintain the rule of law. For that reason, Mosley's rule and *Spencer*, plus the Snowden revelations, might have alarmed the intelligence agencies. CSIS director Jim Judd had indicated in 2008 his concern about "the judicialization of intelligence" or regulatory constraints over Canadian spies (Forcese 2021, 167). In Judd's view, intelligence activities should remain out of judicial control as they had always been, but if the judiciary needs to be involved, then it should perhaps work with and for intelligence.

The best chance to legalize illegal surveillance always comes in a time of crisis. The Harper government introduced new anti-terror legislation in October 2014, days after a violent incident on Parliament Hill. A homeless man killed a soldier standing guard by the National War Memorial in downtown Ottawa and entered the Parliament building. He was shot and killed by parliamentary security. The tragedy created momentum for the government to propose Bill C-44, the *Protection of Canada from Terrorists Act.*

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

Bill C-44 codified and legalized CSIS's extraterritorial surveillance power for the first time. It removed territorial restrictions on CSIS activities, opening the door to warrants that apply outside the country and may breach the laws of other countries (Geist 2015). Contrary to shedding light on illegal intelligence activities, the new law claimed the illegality of intelligence activities on foreign soil as being within the country's jurisdiction, invoking privacy law, and unilaterally legalized them within the single-state framework. C-44 was particularly responding to Mosley's ruling for guerilla accountability and the Arar Commission's recommendation, in order to reverse the effects through legislation. The decision by the Federal Court became meaningless for future activities by CSIS, which can continue to task foreign agencies like the NSA to spy on Canadian and other citizens. Moreover, C-44 incorporates judges into the system of illegal surveillance, by having the Federal Court issue warrants that would violate the laws of other countries. Judges are to authorize illegal deeds by Canadian spies abroad. In turn, the spies receive advance immunity if they violate the law outside Canada. Accountability suffers as well as morality. Retrospectively, this would signal serial backlashes from the intelligence agencies, and more inclusion of the judiciary into intelligence brought about in the next phase.

Phase Three: Developing the Law-Making Ability to Stand above the Charter

In 2015, Bill C-44 paved the way to introduce Bill C-51, "the most radical Canadian national security law ever enacted in the post-*Canadian Charter of Rights and Freedoms* period," as Craig Forcese and Kent Roach state (Forcese and Roach 2015, viii). Within a few months after the incident on Parliament Hill, and in the global climate of the attack on the French satirical newspaper Charlie Hebdo in Paris, Bill C-51, the *Anti-terrorism Act* was tabled, in order to keep hitting the legislative target in a time of crisis (ibid.).

This is complex legislation which creates two new laws and amends fifteen others, including the *Criminal Code* and *CSIS Act*. The Canadian Civil Liberties Association summarises it in six broad changes: 1) creating new offences that criminalize the act of knowingly promoting "terrorism offences" while being aware of the possibility that someone *may* commit such an offence, 2) allowing preventive arrest and detention of a person if it is *likely* to prevent a "terrorist activity" that a peace officer reasonably believes *may* be carried out, 3) creating a new concept of "terrorist propaganda" and allowing a judge to order the deletion of such materials from the internet, 4) giving CSIS a new power to take measures to "reduce threats to the security of Canada," even if doing so would violate the *Charter* and laws, 5) allowing government institutions to share information with each other about "activities that undermine the security of Canada," and 6) codifying the minister's ability to put Canadians on a "no-fly list" (CCLA 2015, emphasis in original).

Although every one of these points significantly legalizes previously illegal surveillance activities, the fourth change, giving CSIS a new power to take illegal measures, is clearly an extension of Bill C-44 in endorsing law-breaking practices by intelligence agencies. While C-44 legalizes illegal practices by CSIS agents abroad,

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

C-51 lifts territorial barriers and frees agents to take illegal measures within Canada despite the protections of the *Charter*. There is no longer a traditional line of demarcation between foreign and domestic collection of personal information, meaning that Canadian residents are no longer protected by citizenship from being spied on by intelligence agencies. Along with "the judicialization of intelligence," intelligence agencies have increasingly developed their potential to create favourable legislation for their own interests.

CSIS's law-making ability encompasses the judiciary. Both C-44 and C-51 have similar legal structures to incorporate judges into pre-authorizing illegal activities committed by intelligence agencies and granting them immunity. CSIS obtains warrants for the purpose of reducing threats to Canadian security through secret judicial processes with judges. C-51 makes "judges agents of the executive rather than overseers of the legal propriety of government actions" (Whitaker 2015, 218), and it "transformed the role of the judiciary from a protector of *Charter* rights into a pre-authorizer of *Charter* violations" (Forcese and Roach 2015, 3). In the Five Eyes nexus, this secret court system seems to be imported from the US Foreign Intelligence Surveillance Court, which rubber stamps NSA warrants with one-sided information (Greenwald 2014). It lacks adversarial evidence by the persons under scrutiny and by the public eye. Oversight in secrecy is oversight denied, as Whitaker suggests (Whitaker 2015, 219).

It remains, however, questionable whether giving CSIS this unconstitutional tool strengthens the security of Canada. The term *reduce* threats to Canadian security deserves to be interpreted with extra caution. *Reduce* does not refer to finding and holding terror suspects accountable in the criminal justice system. Rather, it refers to disrupting suspects' acts, for example, using preventive arrests and peace bonds or, as CSIS's precursor demonstrated, the endless, illegal surveillance activities of the 1970s. As Forcese and Roach remind us, "CSIS and police disruptions are no substitute for efficient terrorism investigations and prosecutions leading to convictions" (Forcese and Roach 2015, 9). Since CSIS is not law enforcement, it has repeatedly failed to turn intelligence into evidence that can be used in the criminal courts. Forcese and Roach suggest a consistent imbalance that CSIS has exhibited in overreacting to crimes with illegal, violent activities, and underreacting in collecting evidence to bring criminals to justice. The efficiency of these unconstitutional intelligence methods would never be tested in open courts, and would remain secret.

On the other hand, Bill C-51 stretches the area of national security. The creation of the *Security of Canada Information Sharing Act* codifies an expansive definition of national security about any activities that "undermine the security of Canada." It refers to any activity that "undermines the sovereignty, security, territorial integrity of Canada or the lives or the security of the people of Canada," including activities that "unduly influence" the government and interfere with public safety or the "economic or financial stability of Canada" (CCLA 2015). The broad scope of information, most of which has nothing to do with terrorism and includes almost any kind of information, is shared among CSE, CSIS, and fifteen other government departments and agencies. Those agencies have captured more and more personal data, and security threats tend to fall into forms of dissent (Geist 2015), which

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

should be protected by *Charter* rights. The secretive sharing of personal data, again, ignores and reverses the Arar Commission's recommendation on rigorous handling of data with reliability, relevance and accuracy.

It is also worth noting that the first point in the CCLA's summary of C-51, criminalizing the act of knowingly promoting "terrorism offences," shows a striking commonality with Japan's *Conspiracy Act,* which criminalizes communications on committing a crime. The crime does not need to be actually committed, but a possibility that someone *may* commit such an offence is in itself sufficient to be a crime. In this sense, counter-terror law is commonly preemptive, attacking potential suspects in the future tense, which inevitably runs counter to the suspect's presumed innocence until proven guilty. This immediately leads to the CCLA's second point, preventive arrest and detention, if someone, again, *may* carry out a plan. Both changes bring a lower threshold of evidence because of uncertainties about the future, seen in the languages of "may" or "likely." The third point, about deleting "terrorist propaganda" from the internet, also extends the range of terror crime, and conflicts with freedom of expression. Above all, these points reflect the *Conspiracy Act,* although preventive arrests are still illegal under Japanese law. Canada's *Anti-Terrorism Act* of 2015 can be the next model exported from the Five Eyes to Japan, or to any other countries in the international circle of policy laundering.

And last, but not least, the creation of the *Secure Air Travel Act* by C-51 verifies intelligence agencies' law-making ability. The *Secure Air Travel Act* codifies the ability of the Minister of Public Safety and Emergency Preparedness to put Canadians on a "no-fly list." But, banning people whose names are on secret lists from boarding international and domestic flights in Canada has been long practiced since the aftermath of 9/11. The new law formalizes this highly arbitrary system that has disproportionally targeted people with Arabic names without contributing any clarity to the process. Rather, the details remain completely secret: who is on the list, how many are on it, and for what reasons and based on what evidence they are denied the right to travel by plane (ICLMG 2020).

Therefore, Bill C-51 certainly brought the judicialization of intelligence, but in a way very favourable for intelligence. Intelligence agencies saw unprecedented triumph as a law-making force and an extrajudicial power. At first, they began practicing illegal surveillance, based on their secret interpretations of law and order. Then, their illegal practices were converted into law. In this way, they can keep pushing legal boundaries for their illegal activities, and the new laws keep granting eternal impunity in the guise of the rule of law in a democratic jurisdiction. The trick is that intelligence agencies strongly influence all three government branches (legislative, executive and judiciary).

The totalitarian character of Bill C-51 invoked a wide range of civil coalition and protest. The bill was eventually amended and enacted in June 2015, but the Conservative government lost in the following national election (Nesbitt 2020). The winning Liberal party promised to repeal the "problematic element of C-51" and add effective oversight. To this end, Bill C-59 was introduced in 2017.

For the new oversight, the bill replaced the SIRC with the National Security and Intelligence Review Agency (NSIRA). It would review not only CSIS, but also

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

matters of national security across the government. And it created the Intelligence Commissioner, who oversees both CSIS and CSE (Nesbitt 2020). However, Justin Trudeau's government also added a new power to another intelligence agency, the CSE. It expanded the CSE's mandates in two dimensions: First, CSE provided technical and operational assistance to Canadian Forces and the Department of National Defence, in addition to federal law enforcement and security (Rosati 2019). The CSE's warrantless wiretapping (Mandate A) had already raised a profound accountability question, as the Defence Minister authorizes such interceptions of private communications. Wiretapping is not constrained to specific individuals nor subject matter, and lacks judicial oversight. Second, it created a new mandate to engage in "active cyber operations…to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." Active cyber operations include cyber-attacks that use malware to penetrate computer networks and websites that cause political, military, economic or other types of damage (ibid., 203).

Though Bill C-59 brought greater oversight and review to secret activities by intelligence agencies, the simultaneous, drastic expansion of power for cyber operations obviously marks another milestone in the trend to legalize illegal surveillance. Because the CSE is a foreign intelligence agency, it also raises new tensions in international relations (West 2016). Article 2(4) of the *United Nations Charter* states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the Purposes of the United Nations." This is the principle of non-intervention in state sovereignty, codified in international law, and the UN *Charter* prohibits the use of force. The CSE's new capacities of cyber operation against another state seem to qualify as use of force against state sovereignty. More accurately, Leah West points out that, regardless of whether cyber operations undertaken by CSE amount to a use of force, the operations will very likely violate state sovereignty, because international law does not just prohibit armed or violent intervention, but bans "all forms of interference and attempted threats against the personality of the State or against its political, economic and cultural elements" (ibid., 403). When cyber operations amount to a use of force, the operations may invoke countermeasures from the targeted state, and CSE employees could be seen as combatants. West warns that failure to comply with the international laws of armed conflict can result in the commission of war crimes by the CSE.

In a sense, Bill C-59 supplemented and updated C-51; while C-51 legalized the illegal surveillance at CSIS, C-59 did the same thing at CSE, as if equally authorizing the expansive power of the two major intelligence agencies to stand above the *Charter*.

Conclusion

In summary, Canada has enforced a series of legislations to legalize the previously illegal mass surveillance activities by the national security intelligence agencies in

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

the War on Terror. The government used the Council of Europe's *Convention on Cybercrime* to grant intelligence agencies and law enforcement "lawful access" to internet subscriber information without warrants, in the name of international harmonization. Though the policy laundering was not successful enough to convince the public, a few criminal and social incidents created the opportunities to break through the opposition. Bill C-13, the *Protecting Canadians from Online Crime Act*, allowed the lawful access by the government to internet subscriber information without warrants. Bill C-44, the *Protection of Canada from Terrorists Act*, codified CSIS's extraterritorial power and incorporated the judiciary to authorize illegal activities by CSIS abroad. Against such radical shifts, the Supreme Court ruled that police are still required to obtain a warrant to get subscriber information from providers (*R v Spencer*), and Federal Court judge Mosley ruled illegal that the CSE tasked foreign agencies to conduct interceptions on Canadians.

However, the judicial resistance faced a serious backlash by the intelligence agencies in Bill C-51. The *Anti-terrorism Act* granted CSIS exceptional power to take measures to "reduce threats to the security of Canada" even if doing so would violate the *Charter* and other laws. The following Bill C-59 also extended the CSE's spying activities to aggressive cyber operations. The two overriding laws have implied that intelligence agencies have been instilling and even partially taking over the law-making ability of Parliament, as an extrajudicial power to stand above the *Charter* rights. In parallel, while they did not have legislation for lawful access to internet subscriber information, CSE implemented the metadata collection program by secret ministerial approval and gathered more data than subscriber information. The metadata program represents a recurring pattern that intelligence agencies first practice illegal mass surveillance in secrecy, and then influence lawmakers to rewrite the law to legalize the illegal state activities.

When situating the Canadian legislative trajectory from the transnational perspective, the adoption of similar legal techniques to those used in the United States and Japan are evident. Canada's attempt at lawful access began with policy laundering through the Council of Europe's *Convention on Cybercrime*, signed in 2001, which paralleled Japan's pursuit of the *Conspiracy Act* through the *United Nations Convention on Transnational Organized Crime*. As Japan's *Secrecy Act* was "designed by the United States," the NSA strategically innovates legal tools to circumvent constitutional barriers, and exports and pressures other countries to adopt them, another site of policy laundering. Among the legal innovations, retroactive immunity indicates an ultimate goal for intelligence agencies, as the 2008 *FISA Amendments* allow the government to dismiss lawsuits over a warrantless surveillance program in the United States if the government secretly certifies to the court that the surveillance was authorized by the president. Bill C-44 and C-51 similarly extended the use of secret courts in Canada, which warrants intelligence agencies to spy on citizens based on unilateral evidence. These legal innovations help further the impunity of intelligence agencies. The techniques have been proliferating among the countries that share the ICT infrastructures as the sites of mass surveillance on the global scale.

Of course, every country has a different political culture and historical relation to the United States, while law-making proceeds among many actors behind the

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

scenes, especially in the complexity of national security law and covert intelligence. Perhaps Canada's uniqueness in the process of legalizing illegal surveillance is in the active inclusion of its judiciary, not in the sense that intelligence comes under judicial control, but in the sense that intelligence recruits the courts into authorizing illegal operations. Thus, the expansion of state surveillance simultaneously threatens checks and balances in state power.

The Canadian intelligence agencies continue to push the legislative boundaries in legalizing illegal mass surveillance. However, the transnational analysis reveals that they have hit the outer wall of international law and legal principles, even though manipulating the legal boundaries of national statutes.

Hostile spying activities are inherently illegal in international law. Some Canadian scholars have pointed that out, especially concerning Bills C-51 and C-59, by mentioning their "clear violation of international human rights standards" (Austin 2015, 117) and "[t]he need for robust extraterritorial protection of human rights" (Israel 2015, 87). In addition, hostile spying activities inevitably raise political tensions, not only in adversarial relations, but also among allies. They damage trust in global communities, exacerbating existing tension and leading to conflicts and wars. As the recent tension between the United States and China over technological hegemony escalates, spying activities have only contributed to a spiral of global surveillance competitions, to which citizens and residents of all countries are subjected. Legalizing illegal mass surveillance within single-state statutes is a dangerous game because it brings people towards ever-escalating surveillance and a world in perpetual conflict, with jingoistic nationalism blocking the view to the common, harmful effects of illegal mass surveillance over the global population.

The transnational perspective also suggests that nobody in any country should be subjected to illegal mass surveillance. An international framework to regulate illegal mass surveillance is necessary, to undo law-making by intelligence agencies, reestablish the rule of law, and protect people's human rights to privacy and expression. This will in turn help create a more peaceful political relation that does not need invasive mass surveillance among countries. Privacy and data protection law also obtain real teeth when they go beyond a single-state regime.

References

American Civil Liberties Union (ACLU). 2005. ACLU Announces international project to stop "policy laundering." April 13. https://www.aclu.org/news/aclu-announces-international-project-stop-policy-laundering?redirect=technology-and-liberty/aclu-announces-international-project-stop-policy-laundering

Angwin, Julia, Jeff Larson, Charlie Savage, James Risen, Henrik Moltke, and Laura Poitras. 2015. NSA spying relies on AT&T's "extreme willingness to help." *ProPublica*. August 15. https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help

Archick, Kristin. 2006. *Cybercrime: The council of Europe convention*. Washington DC: Library of Congress Congressional Research Service.

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

Austin, Lisa. 2015. Lawful legality: What Snowden has taught us about the legal infrastructure of the surveillance state. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. Michael Geist, 103–25. Ottawa: University of Ottawa Press.

Bamford, James. 2001. *Body of secrets: Anatomy of the ultra-secret national security agency: From the cold war through the dawn of a new century*. New York: Doubleday.

Bennett, Colin J., and Charles Raab. 2006. *The governance of privacy: Policy instruments in global perspective*. Cambridge, Mass.: MIT Press.

Bennett, Colin J., Kevin D. Haggerty, David Lyon, and Valerie Steeves. 2014. *Transparent lives: Surveillance in Canada*. Edmonton: AU Press, Athabasca University.

Canadian Civil Liberties Association (CCLA). 2015. Understanding Bill C-51 in Canada: The Anti-Terrorism Act, 2015. May 19. https://ccla.org/understanding-bill-c-51-the-anti-terrorism-act-2015/

Clement, Andrew, Jillian Harkness, and George Raine. 2021. Metadata—both shallow and deep: The fraught key to big data mass state surveillance. In *Big data surveillance and security intelligence: The Canadian case*, ed. David Lyon and David Murakami Wood, 253–68. Vancouver: UBC Press.

Clement, Andrew, and Jonathan A. Obar. 2015. Canadian internet "boomerang" traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. Michael Geist, 13–44. Ottawa: University of Ottawa Press.

Convention on Cybercrime. 2001. Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Electronic Frontier Foundation. n.d. *Hepting v. AT&T*. Accessed April 13, 2022. https://www.eff.org/cases/hepting

European Digital Rights. 2015. Italy: Anti-terrorism decree to strengthen government surveillance. April 22. https://edri.org/our-work/italy-anti-terrorism-decree-strengthen-government-surveillance/

Forcese, Craig. 2021. Bill C-59 and the judicialization of intelligence collection. In *Big data surveillance and security intelligence: The Canadian case*, ed. David Lyon and David Murakami Wood, 167–79. Vancouver: UBC Press.

Forcese, Craig, and Kent Roach. 2015. *False security: The radicalization of Canadian anti-terrorism*. Toronto: Irwin Law.

Freeze, Colin. 2013. How Canada's shadowy metadata-gathering program went awry. *Globe and Mail*, June 15.

Geist, Michael. 2015. Why watching the watchers isn't enough: Canadian surveillance law in the post-Snowden era. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. Michael Geist, 225–56. Ottawa: University of Ottawa Press.

Gellman, Barton. 2013. U.S. surveillance architecture includes collection of revealing internet, phone metadata. *Washington Post*, June 15, 2013.

Greenwald, Glenn. 2014. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Toronto: Signal.

Hiraoka, Hideo. 2018. Was the conspiracy offence necessary for anti-terror measure and toc convention? In *Conspiracy Act Kommentar* (共謀罪コンメンタール), ed. Shinichiro Koike, Yoko Yonekura, and Daisuke Yamada, 182–89. Japan: Gendai Jinbun Sha.

Huey, Laura, and Richard Rosenberg. 2004. Watching the Web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice* 46 (50): 597–606.

International Civil Liberties Monitoring Group (ICLMG). 2020. Time to end Canada's no fly list once and for all. November 5. https://iclmg.ca/time-to-end-no-fly-list/

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

Israel, Tamir. 2015. Foreign intelligence in an inter-networked world: Time for a re-evaluation. In *Law, privacy and surveillance in Canada in the post-Snowden era*, ed. Michael Geist, 71–101. Ottawa: University of Ottawa Press.

Kaido, Yuichi. 2017. What is the conspiracy crime? The forthcoming surveillance society that takes away our freedom. In *Conspiracy Crime for Beginners (*一からわかる共謀罪*)*, ed. Abolish the Secrecy Act Committee, 4–11. Japan: Abolish the Secrecy Act Committee.

Klein, Mark. 2009. *Wiring up the big brother machine… And fighting it*. Charleston, SC: BookSurge.

Lyon, David. 2007. *Surveillance studies: An overview*. Cambridge, UK: Polity.

Lyon, David, and David Murakami Wood. 2021. Introduction. In *Big data surveillance and security intelligence: The Canadian case*, ed. David Lyon and David Murakami Wood, 1–18. Vancouver: UBC Press.

Nesbitt, Michael. 2020. Reviewing Bill C-59, *An Act Respecting National Security Matters 2017*: What's new, what's out, and what's different from Bill C-51, *A National Security Act 2015*? *School of Public Policy Publications* 13 (12): 1–31.

Ogasawara, Midori. 2017. Surveillance at the roots of everyday interactions: Japan's conspiracy bill and its totalitarian effects. *Surveillance & Society* 15 (3/4): 477–85.

Ogasawara, Midori. 2021. Collaborative surveillance with big data corporations: Interviews with Edward Snowden and Mark Klein. In *Big data surveillance and security intelligence: The Canadian case*, ed. David Lyon and David Murakami Wood, 21–42. Vancouver: UBC Press.

Palfrey, Terry. 2000. Surveillance as a response to crime in cyberspace. *Information & Communications Technology Law* 9 (3): 173–93.

Parsons, Christopher. 2015. Stuck on the agenda: Drawing lessons from the stagnation of "lawful access" legislation in Canada. In *Law, privacy and surveillance in Canada in the post-Snowden era*, ed. Michael Geist, 257–83. Ottawa: University of Ottawa Press.

Rosati, Nicholas. 2019. Canadian national security in cyberspace: The legal implications of the communications security establishment's current and future role as Canada's lead technical cybersecurity and cyber intelligence agency. *Manitoba Law Journal* 42 (4): 189–205.

Rudner, Martin. 2002. Contemporary threats, future tasks: Canadian intelligence and the challenges of global security. In *Canada among nations 2002: A fading power*, ed. Norman Hillmer and Maureen Appel Molot, 141–71. Don Mills, ON: Oxford University Press.

Starosielski, Nicole. 2015. *The undersea network*. Durham, NC: Duke University Press.

United Nations Charter. 1945. https://www.un.org/en/about-us/un-charter/full-text

United Nations Convention against Transnational Organized Crime. 2000. https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

Webb, Maureen. 2007. *Illusions of security: Global surveillance and democracy in the post-9/11 world*. California: City Lights.

West, Leah. 2016. Cyber force: The international legal implications of the communication security establishment's expanded mandate under Bill C-59. *Canadian Journal of Law and Technology* 16 (2): 381–421.

Willsher, Kim. 2015. France approves "big brother" surveillance powers despite UN concern. *Guardian.* July 24.

Whitaker, Reg. 2015. The failure of official accountability and the rise of guerrilla accountability. In *Law, privacy and surveillance in Canada in the post-Snowden era*, ed. Michael Geist, 206–24. Ottawa: University of Ottawa Press.

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press

Case law

R v Spencer, 2014 SCC 43.

Legislation

Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Sess, 41st Parl (Canada). https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/

Bill C-44, *Protection of Canada from Terrorists Act*, 2nd Sess, 41st Parl (Canada). https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_9/

Bill C-51, *An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, 2nd Sess, 41st Parl (Canada).

Bill C-59, *An Act respecting national security matters,* 1st Sess, 42nd Parl (Canada).

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Conspiracy Act, An Act to revise the Organized Crime Punishment Act (Japan) 2017. http://www.moj.go.jp/content/001221006.pdf

Foreign Intelligence Surveillance Act [FISA] of 1978 Amendments Act of 2008 (United States) 2008. https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf

Secrecy Act, Act on the Protection of Specially Designated Secrets (Japan) 2013. http://www.japaneselawtranslation.go.jp/law/detail/?id=2543&vm=04&re=01

Midori Ogasawara
Department of Sociology, University of Victoria
mogasawara@uvic.ca

https://doi.org/10.1017/cls.2022.9 Published online by Cambridge University Press