Part Three
Digital Politics
In late spring and summer of 2013 the *Guardian* newspaper (U.K.) published a series of stories detailing massive and previously unknown surveillance by the United States National Security Agency (*NSA*). The stories were triggered by leaks from former *NSA* contract employee and whistleblower Edward Snowden, who himself became the target of a worldwide U.S. manhunt. These revelations triggered a cascade of other stories about the extent of secret *NSA* surveillance programs that went beyond the authority of the Foreign Intelligence Surveillance Act (*FISA*). What was stunning for many observers was that massive amounts of electronic data were being collected indiscriminately and without a warrant on most Americans and millions of persons living in countries overseas. Chronicling the activities of *NSA* is beyond the scope of this chapter, but suffice it to say it clearly went well beyond its mandate, and demonstrated that national security risks were not limited to select targets but were becoming globalized to include entire populations or very large subsections of them.

While the revelations about the scope of *NSA* surveillance surprised many, for others they were consistent with longer term trends. For years, Balkin and
Levinson claim, the U.S. government has been busy constructing the “National Surveillance State”:

This National Surveillance State is characterized by a significant increase in government investments in technology and government bureaucracies devoted to promoting domestic security and (as its name implies) gathering intelligence and surveillance using all of the devices that the digital revolution allows. (2006: 131)

The National Surveillance State (NSS) is, I argue, the logical culmination of what Giorgio Agamben (2007) describes as the “state of exception” (or emergency) that governments employ during times of crisis. Here digital technologies appear not as technologies of freedom but as technologies of control. In this chapter I discuss the rise of the NSS and the threat it poses to the Internet, democracy, freedom, privacy, and human rights, comparing its development in the United States, United Kingdom, Australia, and Canada. The NSS is not particular to Anglo-American liberal democracies; it has become globalized, with states networked and working together on common standards of data gathering, surveillance, and information exchange. Increasingly, however, the NSS is being viewed with alarm and is now facing resistance that is intensifying, globalizing, and meeting with a degree of success.

Agamben’s work provides insight into the National Surveillance State’s establishment and operation in the U.S. context. While surveillance is omnipresent in society, the dominant actor in surveillance, in both scale and sophistication, is the state. Moreover, with the NSS, it is the executive that dominates all other parts of the government apparatus. Legislatures are continuing to wane in their importance, while at the same time providing a veneer of legitimacy to state surveillance. The latest developments of the NSS in the United Kingdom, Australia, and Canada provide a comparative context for the U.S. version. Here it is important to understand that while each state is attempting to territorialize the Internet they do so under the auspices of international agreements such as the Budapest Convention on Cybercrime (2001) and the European Union Data Retention Directive (2006). As state surveillance becomes more invasive, however, resistance is spreading as well. In the midst of this mounting confrontation, the following questions arise. Is the National Surveillance State a given? Can we only hope to make it more benign? What are the implications for democracy? Freedom? Privacy? Human rights?
THE NATIONAL SURVEILLANCE STATE

According to Balkin and Levinson, the National Surveillance State (NSS) began emerging in the aftermath of 9/11, which created a global moral panic leading to countries around the world passing new surveillance legislation. Lyon observes that these laws “tend to relax the limitations on previously stricter laws, such as those to do with wiretapping or indeed any message interception” (2004: 143). In an environment of perceived threats the state responds by “taking action in the online environment to secure national interests in a global network” (Birnhack and Elkin-Koren, 2003: 16). Accordingly the state “implements its ancient duty of securing individual safety and national security. In this context the digital environment is perceived as threatening national security” (Birnhack and Elkin-Koren, 2003: 16).

While the focus of Balkin and Levinson is on the NSS as a contemporary phenomenon, it has both ancient and modern antecedents, explored in Agamben’s work on the “state of exception” (emergency). The state of emergency has its roots in Roman law and has become part of the constitutional fabric of most modern states. In an act of self-preservation the sovereign (state) can declare a state of emergency whereby the “normal law” of the state is not abolished but suspended in terms of application. The law, however, technically “remains in force” (Agamben, 2007: 31). The state of emergency, in brief, represents a space without law: a “threshold of indeterminacy between democracy and absolutism” characterized by sweeping grants of power by the legislature to the executive (2007: 3).

The state of emergency has historically been imposed in wartime and suspended thereafter. In the twentieth century, the state of emergency has expanded to include economic or labour crises, and today, the unending “War on Terror.” According to Agamben, “the state of emergency tends more and more to present itself as the dominant paradigm of government in contemporary politics” with deep roots in the political and legal fabric of the state (2006). A report commissioned by Congressional Research Services acknowledged the extent to which national emergency law had become “rooted in statutory law” (Relyea, 2007: 21). According to the report:

Under the powers delegated by . . . Congressional statutes, the President may seize property, organize and control the means of production, seize commodities, assign military forces abroad, institute martial law, seize and control all transportation and communication, regulate the
In controlling the lives of citizens, the report is alluding to the biopolitical power of the state to target and isolate certain subsections of the population, for example, foreigners, by means of detention (for instance, Japanese Americans during WWII) or surveillance. Today, in the aftermath of 9/11 the state of emergency is becoming prolonged. Furthermore, Agamben claims “history teaches us how practices first reserved for foreigners find themselves applied later to the rest of the citizenry” (2004a). These practices include digital means of surveillance, which have now “reached previously unimaginable levels” (2004a). As the state of exception becomes normalized the population of the state itself comes under suspicion and surveillance. Indeed, as this chapter will show, targeting entire populations is becoming increasingly common. As the state of exception becomes total and normalized, it thus radically changes the relationship between state and citizens to one of state and suspect.

It is the United States that took the lead in governing the hostile environment of the post 9/11 world. Congress passed a variety of pieces of legislation giving the executive sweeping powers to identify, detain, and conduct surveillance on foreigners. These include the Patriot Act in 2001 and the Foreign Intelligence Surveillance Act in 1978 (FISA), amended in 2007 and 2008, along with other pieces of legislation. By the latter part of the twentieth century the U.S. had at its disposal a wide range of new means of surveillance that it was employing against a host of perceived threats stemming from the Internet. While the “War on Terror,” the basis for the ongoing “state of exception,” is the primary factor in the creation of the NSS, the availability of these technologies made it almost inevitable that they would be more widely used on the population as a whole.

While the U.S. has a host of agencies such as the NSA that conduct surveillance on its population, they rely upon the private sector for much of their data. Today, thanks to the leaks by Edward Snowden, much more is known about how widespread this illegal practice is. One NSA program, PRISM, permits top-secret direct access to servers of Facebook, Google, Apple, and Skype, among others, allowing “officials to collect material, including search history, the content of emails, file transfers, and live chats” (Greenwald: 2013a). PRISM, however, was just the tip of the iceberg in terms of the massive surveillance and widespread violation of the law by the NSA.
Surveillance increases the power of governments. As Lyon notes, “whatever the purpose of surveillance . . . power is generated and expressed by surveillance” (2009: 453). This, in turn, encourages the state to invest more in the means of surveillance, thus potentially amplifying the power of the state. The result, Ogura argues, is that the surveillance state is leading to the decline of the rule of law. “Law,” he argues, “is directed at the regulation of human behavior, but it cannot control computers” (2006: 286). What controls computers are code and protocol and these can be used to mask human agency and avoid the rule of law. Furthermore, Ogura asks, “is it rational to suppose that e-government [i.e., the surveillance state] will use ICT lawfully, when it has unlawful capabilities?” (286). The result, now clearly evident in the U.S., is that the rule of law and legislative bodies have a decreasing ability to act as a check on the executive branch.

The legislative branch faces decline, but the NSS still requires the legislative branch to legitimate and bless its expansion. Presciently, Balkin and Levinson argue that the NSS was the product of bipartisanship between the Democrats and Republicans, and that any president replacing Bush would continue the same policies. Indeed, as we shall see in the next section, the same is true of the United Kingdom, Australia, and Canada. One reason for this path dependency is that the magnitude of the decisions make them very difficult to undo. Second, discretion and absence of accountability are simply too tempting to ignore. Third, the state of exception has become normalized with the creation of a totalizing means of surveillance.

Indeed, this is precisely the case. In terms of surveillance and its disregard for the formalities of the rule of law and the Constitution, the Obama administration has continued in the same path as the Bush administration, and indeed has exceeded it. In continuing the same surveillance policies, including detention and counter-terrorism activities such as the illegal use of drones to assassinate enemies, American and foreign, Obama is draining these practices of any sense of partisanship. In the fall of 2012 news reports surfaced that the Obama administration had made moves to make the War on Terror permanent (Greenwald, 2012). This not only included the codification of policies on the use of drones for assassination purposes, but also efforts to further entrench the surveillance state.

The National Surveillance State is, then, a long-term project begun under a Republican president, continued and strengthened by a Democratic president, and likely to continue for the foreseeable future unless strong public resistance succeeds in rolling it back. This regime has grave consequences for democracy, civil liberties, the rule of law, and privacy. In terms of the latter, a study by Privacy
International in 2007 put the United States in its black category, keeping company with countries such as China and Russia. The United Kingdom is the other liberal democracy receiving the black label indicative of an endemic surveillance society.

Critical to understand is that the National Surveillance State is a networked state of mutual assistance and learning, with a diffusion of common standards coming from an international treaty and a European Union directive. The primary concern is that these standards impose intrusive surveillance powers, with insufficient legal protections or judicial oversight. The first of these measures is the Convention on Cybercrime drafted by the Council of Europe (COE), with the support of the United Kingdom, Canada, Japan, South Africa, and the United States, and adopted in 2001 (Vatis, 2010). As of October 2010 thirty states had signed, ratified, and acceded to the convention, which permits and encourages any country to ratify it. These did not include Canada, the U.K., or Australia, who only in 2011 and 2012 had begun the process of ratification. The United States ratified the convention in 2006.

The convention has a number of provisions that concern advocates of privacy. They include such provisions for the purposes of law enforcement as:

- Retention of specified computer data of subscribers by Internet service providers
- Requiring ISPs and telecommunications providers to produce subscriber metadata [Article 18(3)]
- The collection of content data by ISPs in real time in certain circumstances.

The convention also requires states to cooperate and render mutual assistance to another state, including employing means of surveillance to enforce cybercrimes of another country, even if that act is not illegal in its own territory or the state does not adhere to democratic norms.

The Convention on Cybercrime has proven to be controversial. Equally controversial has been the European Union Data Retention Directive adopted in 2006 and strongly supported by the U.S. and the U.K. (EFF, 2011). The Directive requires all ISPs and telecommunications providers to keep all metadata for a period of six months to two years, depending on the member state (Bignani, 2007). The Directive is facing constitutional challenges in a number of European countries, but its principle of data retention has been proposed in the U.K. and Australia, with Canada conforming more to the Convention.
THE UNITED KINGDOM AND THE NATIONAL SURVEILLANCE STATE: THERE OR ON THE WAY?

This section, and the ones to come on Australia and Canada, profiles each country in terms of growing emphasis on state surveillance, focusing on legislation proposed or introduced in 2012 that indicates the intent to place the entire population of each state under suspicion and surveillance. Prior to the analysis of these latest developments some background and context is provided on surveillance and the War on Terror for each country. These developments have not come without resistance in each country, a phenomenon examined as well.

Background: United Kingdom
The 9/11 attack also created a moral panic in the United Kingdom. Many of the legislative changes that resulted, Wong argues, provide “an interesting parallel to the changes to U.S. law and policy.” Wong claims that overall the U.K. “trend appears to parallel that in the U.S., i.e. to consolidate and enhance government surveillance powers, at least where national security and other fundamental public interests are at stake” (Wong, 2006: 216, 223). Fenwick and Phillipson characterize these powers as “draconian” and “authoritarian” (2007: 457, 458). There are some critical differences, however. Unlike the U.S., which took a largely military approach to combating terrorism, the U.K. government approach is police-based (Fenwick and Phillipson). In certain areas the U.K. has gone further than the United States. Although closed circuit television cameras (CCTV) have been in place in the U.K. since the 1980s, there has been an explosion of their presence in the past decade. The result is that there are over 4.2 million surveillance cameras in the U.K., one for every 14.2 people, with the possibility that a person may be recorded over 300 times a day (Wood and Ball, 2006: 6, 7). Their presence is becoming ubiquitous in all locations of the state, including secondary schools and academies (Big Brother Watch, 2012a).

In 2006 the U.K. Parliament introduced a mandatory national ID card with fifty categories of information on each person. The cards provided government agencies vast amounts of information unrelated to fighting crime, terrorism, and the delivery of public services, including what hotels a person stayed at in the U.K. Initially national ID cards were strongly supported by all parties (and the national press), but at the time of passage Labour had to rely on its majority to pass the bill due to growing public resistance. This resistance eventually led
the newly elected Conservative Liberal-Democratic coalition to repeal the act in 2011, although it was retained for foreign nationals outside the U.K.

By the middle of the decade the growth of a surveillance state, and equally so a surveillance society, was meeting with mounting criticism. A 2006 report stated “we are already living in a surveillance society” (with a heavy state presence), which had been growing at an alarming pace since 9/11 (Wood and Ball, 2006). In 2009 a House of Lords committee report noted: “There has been a profound and continuous expansion in the surveillance apparatus of both the state and the private sector.” Moreover, “successive U.K. governments have gradually constructed one of the most extensive and technologically advanced surveillance systems in the world.” The report claimed that the widespread expansion of surveillance by the state was posing “a significant threat to personal privacy and individual freedom” (2009: 5, 26). Concern was expressed that widespread surveillance was changing the relationship between citizen and the state to one of mutual distrust. One witness to a parliamentary committee warned:

Mass surveillance promotes the view . . . that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted. (Norris, quoted in report, 27)

According to Ogura this perspective by the state (and the private sector) is consistent with a “modern/postmodern surveillance-oriented society rooted in a deep skepticism of humans . . . and assumes . . . that being human lies at the root of uncertainty” (2006: 277).

ON TO TOTAL SURVEILLANCE?

The foregoing, as well as the work of Agamben (2004a; 2004b; 2005), suggests that state surveillance would not be limited to target populations, but rather that the entire population would be seen as a source of risk. Indeed, this is the thrust of two proposed changes in legislation, first under Labour in 2008, and later under the Conservative/Liberal-Democratic coalition in 2012. In 2008 the Labour government announced plans to introduce the expected Communications Data Bill, which would create a massive national centralized database that would retain data gathered from Communications Service Providers (CSP). The metadata would include every phone number a person dialed, every website visited, addresses of e-mails sent, and all social media contacts. Use of the data would not
be limited to terrorism or organized crime but would be expanded to include all law enforcement (Open Rights Group, 2012a).

The bill was being proposed to conform to the EU Data Retention Directive, of which the U.K. had been a prime proponent, an interesting circular logic. The Labour government’s proposed legislation would retain communications data for a period of one year. Labour dropped the program after negative responses by the public and service providers. Notably, the opposition also condemned it. The Conservatives opposed the government’s plans, and in a report promised to take a very different approach to surveillance, stating:

Labour has excessively relied on mammoth databases and wide powers of data-sharing, on the pretext that it will make government more effective and the citizen more secure. Its track record demonstrates the opposite, with intrusive and expensive databases gathering masses of our personal information—but handled so recklessly that we are exposed to greater risk. . . . We believe that your personal information belongs to you, not the state. (2009: 1)

These promises soon proved to be hollow, for not long after their election in 2010, the Cameron-led Conservative-Liberal Democratic coalition government began to backpedal on their promises. In 2012 the government introduced draft legislation for discussion, paralleling what Labour had been planning, with one notable difference: that service providers would be required to collect and store the data, not the state. Again, data retention was at the heart of the proposed legislation, the Draft Communications Data Bill. In brief, the government was introducing a nationwide surveillance regime that would log nearly everything the British did online for a period of up to one year. The legislation was needed, the government claimed, to fight terrorists and criminals and protect children from pedophiles.

Even before the legislation was introduced it was criticized both at home and abroad. The conservative Telegraph published several articles sharply criticizing the government’s plans (Whitehead 2012). In response to criticism the draft bill underwent prelegislative consultations by a joint committee of the British House of Commons and Lords in the summer of 2012. Oral evidence and written submissions were extensive, but the most extensive commentary and criticism came from a network of privacy organizations.

The hub of this network is the Open Rights Group. It was joined by such groups as Privacy International, Big Brother Watch, NO2ID, and the Global Network Initiative (GNI), among others, in appearing before the joint
parliamentary committee. Of particular concern was that surveillance would no
longer be targeted but expanded to include the entire population. Big Brother
Watch expressed their concern to the joint committee as follows:

This Bill ends the presumption of innocence as we know it. It represents
a shift of targeted surveillance of those under suspicion . . . to surveil-
lance of the entire populous just-in-case some of them eventually
commit crimes. (Written Evidence, 2012b: 63)

Here Privacy International concurred, warning that the vast expansion of
surveillance “would create a situation in which everyone communicating in
the U.K. would effectively be treated as a potential criminal suspect” (Written
Evidence: 482). The Open Rights Group also expressed concern that the Bill
would “result in a generalized surveillance of the population” (2012b, Written
Evidence: 448).

The concern about privacy was a recurring refrain in the oral testimony and
written submissions to the joint committee. Some privacy critics asserted that
the dichotomy claimed by the government between contact (the source of meta-
data) and content was a false one. It was argued that profiles could be created
on individuals and that mass data collection would mean that “the data could
identify a protester who posts to a radical politics site, and their location at any
given time” (Open Rights Group, 2012b; Written Evidence: 456). The result could
be a chilling panoptic effect on the behaviour of anyone using digitized means
of communication.

Finally, concern was expressed about the assertion of surveillance require-
ments for foreign service providers. Requiring foreign service providers to
identify all their U.K. users and collect data on them, providing it to U.K. author-
ities as requested, could have unintended consequences, set a bad precedent,
and have grave implications for freedom of speech and privacy rights (Global
Network, Written Evidence: 203).

The joint committee appeared to have received the message that the pro-
visions of the bill were excessive, stating the Draft Bill must be “significantly
amended to deliver only necessary data that law enforcement needs” (Report,
December 2012). Lord Blencathra, chair of the joint committee, stated: “We are
very concerned at how wide the scope of the Bill is in its current form” (Report,
December 2012). Whether this will translate into significant changes by the gov-
ernment is another question. Certainly, while the public had severe misgivings
(Ashford, 2012), the PM remained committed to giving police and security services
new powers to monitor Internet activity, despite criticism of current plans (Public Service.Co.UK, 13). However, coalition partner and Liberal-Democratic Deputy Prime Minister Nick Clegg insisted that the Communications Data Bill was dead, stating: “What people dub the snooper’s charter, that is not going to happen—certainly with Lib Dems in government” (Clegg, 2013). The result, for now, would appear to be a stalemate.

AUSTRALIA: FOLLOWING IN THE FOOTSTEPS OF BIG BROTHER, THE U.K.?

Again, like other parts of the world, 9/11 led Australia to pass an onslaught of new laws establishing as primary responsibilities of the federal government national security and the combatting of threats of terrorism. Overall, there was an avalanche of antiterror legislation between 2001 and 2011, fifty-four pieces in all, an extraordinary amount of legislation (Institute of Public Affairs, 2012: 3). The comparison with Canada in this regard is striking. For example, by 2007 Canada had “only enacted two major pieces of anti-terrorism legislation since 11 September, 2001 . . . while Australia . . . enacted close to 40 pieces of such legislation” (Roach, 2007: 53). Australia’s response put the country in a league of its own, exceeding the United Kingdom, the U.S., and Canada. Moreover, “these laws attracted bi-partisan agreement and were enacted with the support of the Labor opposition” (Williams, 2011: 1145). Most of the legislation was passed under the (conservative) Liberal-National coalition government led by John Howard. The Howard government, in fact, passed a new antiterror statute every 6.7 weeks after 9/11, compared to six pieces of legislation during the Rudd and Gillard governments from 2007 to September 2011, which refined, but did not wind back, the Howard government legislation (Williams, 2011).

The passage of such a high volume of legislation that permitted access by law enforcement agencies to the content of email, SMS, and voice mail messages stored by a service provider (but only under warrant) was often done in rushed circumstances. However, unlike during World Wars I and II, when national security legislation was passed and ceased to operate on the cessation of hostilities, the Australian government has consistently stated that “the threat of terrorism to Australia is real and enduring,” that is, the state of exception is permanent (quoted in Williams, 2001: 1138). According to Williams, “It is now clear that the greater body of this law will remain on the Australian statute book for the foreseeable future” (2011: 1171). One outcome of the legislation is that it has shifted the
balance of power to the executive. The result may be that Australia’s democratic freedoms and the rule of law are in danger (Williams, 2011).

**Current Developments**

Australia’s antiterror legislation has been influenced by external forces and precedents (Roach, 2007). Indeed, there is a convergence between Australia’s recent proposal to create a massive national surveillance system, and what was discussed earlier in the U.K. However, the U.K. is not the only source of inspiration. Australia intended its proposed legislation to be a means of both ratifying the Convention on Cybercrime discussed previously (Rodriguez, 2011), and conforming to the EU Data Retention Directive (DRD) (Bowe, 2012).

The DRD was particularly influential in shaping Australia’s national surveillance policy. In June 2010, the Labour-led coalition government admitted that it had “been looking at the European directive on data retention, to consider whether such a regime is appropriate with Australia’s law enforcement and security context” (Grubb, 2010). Almost immediately a Senate Standing Committee began investigating the issue of data retention, recommending in 2011 that the government consult with stakeholders and only retain data necessary for law enforcement. In July 2012 the Attorney-General’s Department released a discussion paper, “Equipping Australia against Emerging and Evolving Threats,” and soon after a Parliamentary Joint Committee on Intelligence and Security began public consultations.

The discussion paper’s focus was clear, stating: “The common thread of national security runs through the proposals, which seek to respond to threats from international state and non-state based actors, terrorism, serious and organized crime and cyber crime” (“Equipping Australia,” 2012: 4). The discussion paper is an extensive document with eighteen primary proposals and forty-one individual reforms. Criticism, however, has primarily focused on the issue of data retention, with the discussion paper proposing “tailored data retention periods for up to 2 years” (11). Of significance as well was the proposal to “enable the disruption of a computer” (11) which would permit “law enforcement to add, delete, or modify any software or data on a computer system in order to execute a computer access warrant,” possibly including the planting of Trojan horse software, keystroke logging, malware or other privacy invasive software on a targeted computer (Pirate Party Submission, 2012a). All this would be done in a new system of warrant control providing greater ministerial discretion over
warrants (“Equipping Australia,” 2012). This would bring Australian legislation in line with what the U.K. had proposed.

In particular, it is the data retention proposal that has been the lightning rod for public criticism. Critics such as Green Senator Scott Ludlam stated data retention was “premised on the unjustified paranoia that all Australians are potential criminal suspects” (Ludlam, 2012). The Pirate Party maintained that the proposals would “make suspects of us all, destroying once and for all the concept of being innocent until proven guilty by placing everybody under surveillance, regardless of suspicion or need” (Pirate Party Submission, 2012a). The Privacy Foundation claimed the government’s current proposals would, if enacted, “very substantially shift the balance away from privacy, and in favour of a significantly expanded ‘surveillance state’” (Australian Privacy Foundation, 2012:8). As in the U.K., communications service providers would become “agents of government” (7). Critics warned the result of a surveillance state would mean the end of privacy.

The Privacy Foundation warned that the proposals would end the “balance, in a free and democratic society, between law enforcement capabilities and privacy and civil liberties” (2012). The Pirate Party warned that “people under constant surveillance stop behaving like free people; to the detriment of society” (Submission, 2012a: 6).

The government tried to persuade the public that its proposals were not as invasive as thought, echoing a similar distinction made by the U.K. government and the EU Data Retention Directive between contact and content (Roxon, 2012). Critics responded that there was a false dichotomy between contact and content and that contact information could be used to create a profile of every user. Furthermore, the plan to monitor every website visited by every Australian would be like having a government “agent seeing every news story you read, every TV show you watch and every issue you research” (Pirate Party, 2012 b, Supplementary Submission, 7).

The committee hearings concluded in September 2012. At present the proposals are in a legislative limbo, in part because of the controversy they have created. In June 2013 the committee released its final report and punted responsibility back to the government, stating: “If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination” (Australia Joint Parliamentary Committee, xxxiii). The Attorney-General in the Labor government, Mark Dreyfus—a government dependent on the Green
Party for support—stated in response that it “will not pursue a mandatory data retention regime at this time” (Taylor, 2013). The 2013 election brought the Tony Abbott–led Liberal/National coalition to power. So far, the new government has not signaled its intent on introducing new surveillance legislation.

CANADA AND THE NATIONAL SURVEILLANCE STATE

Delayed, if not buried, are the key words for the efforts of the Conservative government in Canada to pass legislation, Bill C-30, in 2012 that would have permitted the government to ratify the Convention on Cybercrime and put Canada on the road to a surveillance state. Bill C-30, in fact, represents only one of several attempts by Canadian governments, Liberal and Conservative, to enact sweeping national surveillance legislation beginning with the Liberals in 2005, a process that may be difficult to permanently derail.

Legislative changes to fight the war on terror have been modest in Canada when compared to the United States, the U.K., and Australia. The Canadian Anti-Terrorism Act (2001) gave the government new surveillance powers for the purposes of combatting terror and the gathering of foreign intelligence, permitting, for example, “warrantless interception of foreign communications” (Lawson, 2012: 74). Beyond that, the Canadian state has relied upon the Personal Information Protection and Electronic Documents Act (PIPEDA), passed in 2000. While PIPEDA is intended to protect the privacy of Canadians in certain circumstances, Internet service providers can voluntarily provide law enforcement agencies subscriber information if it relates to an offence or to national security.

However, for over a decade the Canadian government has been under pressure to enact more extensive surveillance legislation, both internally from Canadian law enforcement agencies (LEA) and externally from the U.S. and the U.K. (Lawson and Valiquet, 2006). In response, in 2005 the Liberal government introduced Bill C-74, the Modernization of Investigative Techniques Act, which had two primary objectives:

- To require ISPs to install interception capabilities that could retain subscribers’ personal information, target specific subscribers, and remove any encryption on data.
- To provide LEA access to subscriber information on request without a warrant or court order.
This information could include metadata that could be used to create profiles of Canadian citizens accessing the Internet. The legislation was strongly criticized by Jennifer Stoddart, the government’s privacy commissioner, and by civil society groups (Valiquet 2006). The bill died when the minority Liberal government was forced to call an election.

In June 2009 the minority Conservatives introduced their own version of Bill C-74, Bill C-47, the Technical Assistance for Law Enforcement in the 21st Century Act, which died on the Order Paper when Parliament was prorogued at the end of the year. In the next session of Parliament the same legislation reappeared but as three separate pieces of legislation. Again, Canada’s privacy commissioners were sharply critical of the proposed legislation (Letter, 2011). These pieces of legislation never made it past first reading when another election was called.

These legislative proposals, Liberal and Conservative, had a number of features in common, including giving LEA greater powers to access “subscriber information” without warrant, requiring ISPs to preserve this information even without prior judicial authorization, and expanding scope to track GPS data by any mobile means. Thus Canada would have joined other countries, such as the United States and the U.K., where “new laws have contributed to an explosion of state surveillance” (Lawson, 2012: 6).

BILL C-30: A LESSON LEARNED OR MERELY ANOTHER ATTEMPT?

With the foregoing as a prelude, one can see that Bill C-30, “An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act,” (otherwise known as the “Protecting Children from Internet Predators Act”), introduced in February 2012, was but the latest effort by Canadian governments, Liberal and Conservative, to move in the direction of a surveillance state. While it was eventually withdrawn and left to die, international pressure on Canada to find a means of acceding to the Convention on Cybercrime has continued. For this reason, it is important to see what the Conservative Government was attempting with Bill C-30.

Bill C-30 was a product of pressure from Law Enforcement Agencies (LEA) (primarily the RCMP and municipal police forces) across Canada and the government’s desire to ratify the Convention on Cybercrime, though the latter was never mentioned in the press. In the only parliamentary discussion on the
bill, Kerry-Lynne D. Findlay, Parliamentary Secretary to the Minister of Justice, stated that Bill C-30:

would allow Canada to ratify the Council of Europe convention on cybercrime. In order for Canada to ratify international treaties, it must first bring its law into conformity with the requirements of the instrument. (28 February 2012)

The bill would have made ISPs part of the state’s surveillance apparatus by forcing them to install equipment that could log the Internet activity of their users and turn over subscriber information to LEA without a warrant. ISPs would also be required to provide back-door access to LEA, permitting remote access in real time to the activities of subscribers. The government could also require that ISPs install any equipment necessary to perform its surveillance functions, thus emulating features of the NSA PRISM surveillance program. In addition, Section 487.0195 permitted ISPs to voluntarily provide to LEA the content of emails and the browsing habits of subscribers. In brief, the distinction between contact and content was dispensed with. This was particularly evident in section 33 of the bill, which would, in Orwellian terms, have allowed the minister to appoint an “inspector” who could access any ISP and take any information that the inspector (Ottawa) desired. As one journalist remarked, “we might as well just put a webcam in our homes and give the minister a link to the live feed” (Kline, 2012). Finally, the legislation provided for preservation of data on ISPs, twenty-one days for domestic violations of the law and ninety days in cases of the violation of a law of a foreign state, substantially less than the countries discussed previously, but given the capacity of the government to access and copy information at any time, the preservation (data retention) requirements may have been redundant.

Criticism had been building in anticipation of the bill with civil society organizations and privacy experts objecting to massive online surveillance (Letter, August 2011), as well as the Information and Privacy Commissioner of Ontario (Cavoukian, October 2011). The maladroit Public Safety Minister Vic Toews, the minister responsible for the legislation, stoked strong criticism when he told an opposition MP that he could “either stand with us or with the child pornographers.” The Internet and mass media lit up with criticism (Harrison and Rodriguez, 2012). Thousands of Canadians signed an online petition and two Conservative Members of Parliament publicly criticized the bill. What probably doomed the legislation were the results of a public opinion poll indicating
that most Canadians were opposed to the legislation, with the strongest opposition coming from Alberta, the Tories' bastion of support (Grenier, 2012). The legislation never made it past first reading. In February 2013 Justice Minister Rob Nicholson pulled the plug on the legislation, saying the government “had listened to the concerns of Canadians on this” (Payton, 2013). This, seemingly, was the end of the matter. However, in late 2013 important aspects of Bill C-30 reappeared attached to new legislation to fight cyberbullying and protect children: Bill C-13. These aspects include requiring Internet service providers to release metadata in their possession to the federal government, as well as a grant of immunity to ISP and telecom companies for disclosing personal data of Canadians in their possession. As of this writing the bill was proving to be highly controversial and had not yet passed Parliament.

CONCLUSION

This essay has focused on only four countries, but clearly what is occurring is a global trend. In a yearly review of state surveillance the Electronic Frontier Foundation made the following observation:

States around the world are demanding private data in ever-greater volumes—and getting it. . . . Several laws and proposals now afford many states warrantless snooping powers and nearly limitless data collection capabilities. (Rodriguez, 2012)

In sum, states are expanding their capabilities to surveil their populations in targeted and wholesale ways.

In the United States Balkin and Levinson are pessimistic, arguing “there is no serious possibility of completely forestalling” the shift to a National Surveillance State (2006: 526). Rather, they argue, the questions are: What type of surveillance state will it be? Can the risks to individual privacy and civil liberties be mitigated? Can measures of accountability and transparency prevent the dangers attendant upon increased powers in the executive branch of government?

One can make a case that the state needs to gather information in a world where dangers and threats may actually exist. Moreover, the state needs to act in concert with others to combat these dangers and threats. Surveillance, per se, is not necessarily bad. According to Wood and Ball, “Surveillance is not a malign plot hatched by evil powers. Much surveillance has good or at least neutral intentions behind it: desires for safety, welfare, health, efficiency, speed and
co-ordination.” The danger thus comes when more and more everyday activities are perceived in terms of risk, and thus “what was previously exceptional security becomes normal” (Wood and Ball, 2006, 4). With normalization of surveillance comes a shift from targeting certain persons as risks to perceiving the entire society as a source of risk.

Agamben himself foresaw the potential of the move from “targeted” or select surveillance of certain persons to “untargeted” surveillance of the entire population. In explaining his refusal to go to the United States in 2004 to speak because it meant he would have to give up his biometric information, Agamben (2005) argued that in his case it would have been analogous to the Nazi use of photos in “occupied countries to locate and record the Jews, thus facilitating their deportation,” an example of targeting a sector of the population. The question Agamben then asks is, “What will happen when a despotic power makes use of the biometric records of an entire population?” He then points out that European countries are, in fact, preparing to move from select biometric supervision of immigrants to imposing it “on all of their citizens.” If this happens the “normal relationship of the State” to its citizens will be one of “generalized suspicion” (Agamben, 2005). In all instances it is the state that has the power to ultimately decide what is “valid” surveillance and what is not.

It is this leap to viewing the entire population as a potential threat and the desire to gather and store data on it that is becoming more evident in state policy and action. Clearly, this is the case in the U.S., although the governments of the U.K., Australia, and Canada have expressed similar intent. One hopeful sign is that, as 9/11 recedes into the background and citizens become more aware of the scope of what governments are doing or trying to do, it becomes more difficult for states to consolidate a perpetual state of emergency based on terror, so useful in controlling their populations. One can see signs of pushback. In July 2013 the first serious U.S. legislative challenge to the administration’s domestic spying infrastructure, a measure to defund covert collection of American’s telephone records, was defeated by a narrow vote of 217 to 205. Previously, such a measure would never have made it to the floor for a vote. Elsewhere, the national ID card proved too unpopular for the U.K. government to maintain, and was scrapped. Later, when it did introduce much the same legislation as the Blair government, the Conservative-led coalition met with a cool, if not hostile, audience. Here minority governments are important as they can stall the progress of invasive surveillance measures. In Canada, for example, a series of minority governments delayed the advance of surveillance legislation. By the time the Conservatives
had a majority the threats and risks of terror and crime no longer had such a purchase on public opinion, and even the spectre of child pornography could not persuade them that the risks to privacy and civil liberties were worth it.

Canada also had developed by this time a history of organizing and using the Internet as a means of resistance. The protracted struggle over new copyright legislation demonstrated that Canadians were concerned about digital issues, the Internet, and privacy. And speak out they did. With most Canadians opposed, and in particular their more libertarian, anti–big government base in Alberta, the Conservatives had to retreat.

However, it is too early to assume that the Conservatives in Canada or in the UK and Labor in Australia have given up on pressing ahead with expanding state surveillance. This is clearly not the case in Canada if Bill C-13 is any indication. If Agamben is right—that the state of exception has become normalized—then this is what should be expected. The power of surveillance technologies may be too tempting to leave alone, international pressure too strong to resist. Another moral panic over security may provide the opportunity to pass once unthinkable legislation consolidating the surveillance state. Even if this is not the case, states have demonstrated an increasing willingness to sidestep the law when it comes to surveillance. Legislatively, rather than wholesale measures, governments may try to proceed by administrative regulation, by dividing legislation into separate pieces, with a long end in view, or by massive omnibus legislation, where surveillance measures become lost among other controversial measures. Clearly, for those who cherish privacy, civil liberties, and democracy, vigilance will be the byword.

NOTES

1 For example, the existence of another NSA programme, X-Keyscore, a complement to PRISM, permits officials, without authorization, to search metadata and the content of just about everything a typical user does on the web, including examining the content of all the websites he or she visits, emails sent and received, and browser searches. Searches can be conducted in real time. NSA also gathers large amounts of metadata on the telephone calls, emails, cell phone text messages and chat transcripts on millions of Germans (Poitras et al., 2013a), tapping indiscriminately into and storing the email of millions of Brazilians (Greenwald, 2013b), and conducts electronic surveillance on European institutions and diplomats (Poitras et al., 2013b). “Metadata” is “the ‘envelope’ of a phone call or Internet communications. For a phone call this could include the
duration of a phone call, the numbers it was between, and when it happened. For an email it would include the sender, recipient, time, but not the subject or content. In both cases it could include location information” (Greenwald 2013c).

REFERENCES


Institute of Public Affairs. 2012. “Submission to Parliamentary Joint Committee on Intelligence and Security on ‘Equipping Australia against Emerging and Evolving Threats.’” https://www.academia.edu/6590064/Submission_to_Parliamentary_Joint_Committee_on_Intelligence_and_Security_on_Equipping_Australia_against_Emerging_and_Evolving_Threats_.


