Surveillance & Society

Debate

The Curious Tale of The Dog That Hasn't Barked (Yet)

Reg Whitaker

University of Victoria and York University, Canada. regwhit@uvic.ca

We begin in the fall of 2001. In the immediate shadow of the 9/11 terrorist attack on the Twin Towers, the Canadian Parliament debated the *Anti-terrorism Act 2001*. Despite its title, this legislation was something of a mini-omnibus bill, a national security act covering a range of security issues beyond terrorism. However, there was one clearly identified gap. Unlike the *USA Patriot Act*, rushed precipitously through the US Congress, the Canadian legislation contained no provisions for enhanced electronic surveillance of internet communication. Instead, the government promised to follow up with further legislation addressing this latter issue, with a nod toward the 2001 European Convention on Cybercrime as a broad set of guidelines. The impression left by government spokespersons was that new communication technologies and a deregulated telecommunications environment required some serious legislative upgrading and modernization of electronic surveillance rules to meet the threat of terrorism and international organized crime. The expectation was that the new legislation would follow expeditiously, although there would be time for public and industry consultation before a final draft was prepared.

Fast forward eleven years to the fall of 2012. Despite two separate rounds of national consultation on what was called in Canadian Orwell-speak, 'Lawful Access'; draft laws that died on the Parliamentary order paper; and finally a 2012 bill that had to be ignominiously withdrawn in the face of vociferous criticism from all sides, Canada remains exactly where it was more than a decade ago with regard to electronic surveillance powers. In the United States, there was controversy over the expanded surveillance powers in the *USA Patriot Act*. Then a few years later investigative journalism revealed that warrantless surveillance was being secretly practised by agencies regardless of the provisions of the law. In response, legislators (including then Senator and now President Barak Obama) hurried to simply rubberstamp the practice *post facto*. In the United Kingdom, where there was a longstanding threat of Irish Republican terror, the pre-9/11 *Regulation of Investigatory Powers Act 2000* provides wide scope for interception and enforced decryption of internet communication in the name of national security, not to speak of various other grounds.

Canada, under both Liberal and Conservative governments, has been a good and conscientious partner of its allies in fighting global terrorism, ready to do what seems to be required, even when this involves wrenching changes to long held Canadian values and ignoring international commitments to protect human rights. For instance, leaked memoranda indicate ministerial level approval of Canadian agencies under certain circumstances permitting the use of information from abroad that might have been gathered by torture and other 'enhanced interrogation' techniques that are abusive of internationally recognized standards. So why has Canada become an isolated outlier in relation to electronic surveillance powers? Are there any wider lessons to be drawn from this unusual position?

Whitaker, R. 2012. The Curious Tale of The Dog That Hasn't Barked (Yet). *Surveillance & Society* 10(3/4): 340-343. http://www.surveillance-and-society.org | ISSN: 1477-7487

Some of the answer to the first question rests simply on circumstance. The passage of the *Anti-terrorism Act* was followed by four successive federal elections within a span of seven years. The first three of these resulted in minority Parliaments with the accompaniment of hyper-partisanship and persistent instability; the second in the defeat of the incumbent Liberals and their replacement by their Conservative rivals; only the fourth election in 2011 resulted in a majority Parliament. There have been three prime ministers over this span and even though the first two were Liberal, the transition between Jean Chrétien and Paul Martin was almost as fraught with political conflict as the later transition from Martin to Stephen Harper. In short, the political landscape was not conducive to easy passage of contentious new powers. Some legislative drafts simply vanished because governments were defeated or snap elections called.

The chaotic political context cannot entirely answer the question of why the dog never barked. A majority Liberal government was still comfortably in place when the Justice Department produced a 'Lawful Access Consultation Document' in 2002 that was submitted to separate rounds of consultation with public stakeholders (civil liberties and privacy advocates, etc.) and telecommunication industry representatives. This process, however, failed to produce a consensus. A second round of national consultation was carried out in 2005. Although any potential outcome of this second go-round was aborted by the defeat of the Liberal government in Parliament in late 2005 and the election of a Conservative minority in early 2006, it is unlikely that any basis for moving ahead had actually been achieved before the political upheaval. In any event, when long effort finally congealed in an actual legislative project before Parliament it was in the context of a stable majority government. The result was an embarrassing debacle and an ignominious retreat by the Tory government.

Some clues to this puzzle can be found in the public consultation rounds. I was a participant in these and can report that the civil society participants were generally sceptical if not downright hostile with regard to the civil liberties and privacy concerns generated by the Lawful Access proposals. Policing and security representatives were favourable but the consensus among civil society people was that the former had failed to make a coherent case for why new and enhanced powers were required, when old ones were still adequate. Obviously new technologies called for modernization and updating of legal language and in some cases perhaps for more extensive scope for warranted searches of data to match the new technological requirements. But the range of new powers being sought raised suspicions that government was seeking a fundamental expansion of its coercive reach into civil society using the pretext of the anti-terrorist panic following 9/11. There is, however, little or no evidence to suggest that this kind of criticism had made any impression on successive governments. To understand the hesitation in moving ahead we have to look elsewhere.

Parallel consultations with the telecom industry were held behind closed doors. There is evidence to indicate that the problem that emerged in this forum had little to do with privacy or civil liberties, but had much to do with the question of who would bear the costs of enhanced internet and telecommunication surveillance. There are two interconnected issues at play here. New technologies present a complex challenge to surveillance; state intervention will necessarily be expensive as counter-measures try to catch up, and keep up, with ever improving technologies. Prior to deregulation of the telecommunications sector, monopolies worked co-operatively in a spirit of public service to provide authorized information to appropriate law enforcement and security agencies; moreover, in an era before the explosion of new communication technologies, costs were relatively low and much of the burden was accepted by companies awarded a monopoly position in law. After deregulation and the emergence of a competitive and more technologically innovative market, telecoms became increasingly unwilling to bear the costs of more expensive surveillance measures. Well before 9/11, telecoms began to consider law enforcement and security services as simply customers rather than non-profit organizations carrying out public duties, and began shifting the costs of surveillance from the private to the public sector. Indeed, telecoms began building a profit margin into their dealings with police and security services even in the execution of court

orders. The Lawful Access proposals raised anxieties among the telecoms about how much of the cost of the contemplated new surveillance measures would be imposed on them.

Lacking consensus, especially in the crucial industry sector, successive governments simply put the Lawful Access project on the back burner where it easily fell victim to the shifting political vicissitudes of the latter part of the decade. Even though law enforcement and security services continued to pressure decision makers about the need to step up internet and telecommunication surveillance in the face of the continuing threat of terrorism and organized crime, not to speak of the need for Canada to keep up with its closest allies, public fears about terrorism were quickly receding as no attacks took place on Canadian soil (unlike Britain where the so-called 7/7 London Underground bombings greatly heightened anxiety levels). A minority Parliament in 2007 for instance 'sunsetted' the controversial powers of investigative hearings and preventive detention in the *Anti-terrorism Act* with no popular outcry. There was clearly no public pressure to force lawmakers to get on with a job promised in 2001 at a time of considerable societal alarm, but which now seemed to be losing its *raison d'□tre*.

With a Conservative majority government in place after the 2011 election, showcasing as one of its highest priorities a law and order agenda that included a tough-on-terrorism subtext, the stage seemed set for finally enacting a version of Lawful Access that might reflect some workable private sector-public sector consensus, even if civil society advocates remained skeptical. But when Bill C-30 landed in the House of Commons on Valentine's Day 2012, pandemonium broke loose. The bill had been renamed, transformed from Lawful Access into something called the *Protecting Children from Internet Predators Act*. For ten years the primary target had been terrorist and organized crime networks. Controlling child pornography had been given at best some passing notice. Public Safety Minister Vic Toews revealed why the sudden change had been made when, weirdly echoing the notorious anti-terrorist maxim of George W. Bush, he told a startled and indignant opposition in the House that they were either 'with us' 'or with the child pornographers.' Mr Toews may have figured that this would intimidate opponents. Instead it poured gasoline on a fire.

It was the content of the bill that really ignited the blaze. Telecoms and internet service providers would be forced to install special surveillance devices to allow government access to a range of information on private usage. Where warrants are required, auditing and monitoring mechanisms are provided. Former Tory Public Safety minister Stockwell Day had promised to ensure that any new intrusive powers would only be exercised under warrants. But under C-30, governments could require *without warrant* the production of information on specified customers including name, address, telephone number and e-mail address, as well as the IP address and local service provider identifier. As one expert has pointed out, this would give police the capacity to scan the crowd at a demonstration to gather the identification of each cell phone and electronic device and then gather from the telecoms and ISPs the names and addresses of everyone so targeted. Since there is no persuasive evidence that police have been unable to gather the information they actually require for legitimate law enforcement purposes, this seems to many to represent disproportionate overreach.

The Tories badly miscalculated the political impact of C-30. They managed to stir up two very dangerous points of opposition. The internet community is one that governments around the world have learned to their chagrin not to mess with. Just a month or so earlier, a huge web campaign had forced the US Congress to back down on proposed legislative controls over the internet. Internet users are alert, technically savvy, and plugged into instant response networks. When governments or dot-coms like Google or Microsoft provoke this community, it reacts like a swarm of angry wasps. Vic Toews poked this nest and the wasps were all over him. A Twitter campaign heaped thousands of satirical tweets on the minister's account informing him of the most mundane aspects of the tweeters' lives—just in case he needed to know. Ontario's Privacy Commissioner backed up the internet campaign by throwing cold water over the entire rationale for the bill and said it should be overhauled.

Perhaps more damaging to the government, C-30 set off a storm of opposition from the one area of Canadian society that matters most to the Conservative party, its own base. This was the same government that had killed the long-gun registry on the claim that it was a Big Brother state intrusion into people's private affairs, and had killed the long-form census on the basis that the state had no right to demand details of people's lives. Now it was offering a bill that seemed to give the state even more intrusive powers. Right-wing commentators attacked the bill; right-wing talk radio shows were buzzing with criticism; and even some backbench Tory MPs spoke out in an unprecedented show of independence in a normally disciplined caucus.

Faced with this barrage of criticism from across the political spectrum, Minister Toews and his government beat a hasty and humiliating retreat. For a time it seemed that a revised bill might reappear on the order paper, but that has yet to happen. Legislation restoring investigative hearings and preventive detention to the anti-terrorism arsenal has been introduced in the House of Commons, indicating that the Harper government has not abandoned draconian legal approaches to counter-terrorism. Yet despite public exhortations by the police chiefs and the Director of CSIS, there seems so far to be little enthusiasm for reviving Lawful Access under that or any other name. Some journalists have pronounced the project dead. Even if some version does arise again, it will surely be in a modified and tamed form given the depth and breadth of opposition the first instance inspired.

The surprising fact is that Canada finds itself in a unique position relative to its closest allies with regard to post-9/11 electronic surveillance in the name of national security. Is Canada's position simply idiosyncratic, or are there any wider lessons to be drawn? We can reject culturist explanations, that Canada is unusually liberal compared to its neighbours: a glance at the policies of the current federal government on almost any issue should be enough to disabuse anyone of that notion. I would offer instead the following reflection. Assuming that Canadian political culture is not in fact widely different from that of its neighbours, the USA and UK, a set of fortuitous circumstances prevented the Canadian government from acting with the same haste as its allies in the face of an apprehended high threat level. As public perception of the terrorist threat has diminished, so has public acquiescence to greatly expanded state surveillance powers. Neither organized crime nor child pornography serve as substitute spectres to frighten the public into giving up more privacy and freedom of expression.

As the imminence of the terrorist menace recedes in both the USA and the UK, we may anticipate stronger resistance to any further demands for enhanced surveillance powers, or perhaps even growing insistence on rolling back some of the powers earlier usurped by the state. The internet community is an influential new actor on the world stage with global reach, capable of very swift and agile response to threats to its autonomy, access to information and freedom of expression. Healthy suspicion of state intervention in communication exists on all sides of the political spectrum. These slumbering giants of resistance were roused in Canada but they exist elsewhere as well.

By accident, despite itself, Canada has demonstrated a model of sorts for resistance movements in other countries.