iStock

Understanding technology, security, and liberty in the modern world

Neil Desai of Magnet Forensics writes that law enforcement and national security agencies in Canada and around the world have an arduous task in understanding new technologies used by criminals, and developing and deploying their own technologies while balancing jurisdictional and civil liberties challenges.

Neil Desai

In laying out his theory on the need for a social contract, Thomas Hobbes described human life in the state of nature as solitary, poor, nasty, brutish, and short. Under such circumstances, mankind had to sacrifice liberty in exchange for the security afforded by the modern state. From that bleak, black and white picture of a feudal society, Hobbes left us to choose between the harsh realities of nature and the security provided by the state's apparatus. The unintended consequence for modern Western liberal democracies of this social contract has been a perpetual state of grey. Governments have had a constant challenge of managing the security expectations of their citizens while respecting their constitutionally guaranteed, democratic rights.

The tension created in striking the right balance between civil liberties and security has been prevalent in the Canadian political discourse in recent times. The latest attacks in Sydney, Paris, and Ottawa motivated by the Islamic State of Iraq and the Levant's (ISIL) hateful propaganda coupled with the gruesome images of the terrorist organization's reign of murder, torture, and the enslavement of those who challenge their dogmatic views of Islam in Iraq and Syria, have shifted the general population's willingness to cede more civil liberties in exchange for more security, or the perception of greater security. A recent poll by Abacus Data shows that 18 percent of Canadians list public safety and terrorism as one of their top three issues. In March 2014, the poll showed only 4 percent responding this way.[1]

The Government of Canada has responded with a suite of legislation to combat the threat of terrorism and other modern public safety challenges. Bill C-51 would ease the restrictions on the sharing of information between federal security agencies to "better detect and act upon threats". Bill C-44, dubbed the *Protection of Canada from Terrorists Act*, passed earlier this year. It increases the powers of Canada's domestic spy agency, the Canadian Security Intelligence Service (CSIS), to share information, operate internationally, and keep its sources anonymous. In 2014, the Government passed C-13, the *Protecting Canadians from Online Crime Act*, which includes new police powers such as warrants for surveillance, as well as the tracking and gathering of personal banking information. The warrants issued for crimes related to terrorism would have longer durations than those pertaining to other categories of crimes.

While there has been some criticism from Muslim community organizations, feeling targeted by anti-terror legislation, and civil liberties organizations, the legislation seems to have widespread support among the general population. While opposition criticism has tempered initial support for C-51, it seems the pendulum and public protest have generally swung towards security and away from liberty.

The great challenge for the government and its security agencies, when they achieve these unprecedented powers, is that they will have to shift from arguing for powers to operationalizing them in a timely fashion to keep Canadians safe. Much of the debate that has gone on in Parliament and elsewhere has remained at the existential level, with little attention paid to what practical capabilities exist for national security and police agencies today and what would practically be unlocked to keep Canadians safe by this new legislation.

Canadians likely expect that security agencies such as CSIS, the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), and the Communication Security Establishment (CSE) – Canada's counterpart to the United States' National Security Agency (NSA) – collect data on suspects of terrorism and other serious crimes using modern technologies. However, information on the tools and tactics used by security agencies has largely been left to the imagination. Activist civil liberties groups in Canada and elsewhere have struck fear that government is overreaching by invoking theories that resemble Hollywood-style, meta-data collectors that could allow security agents to review citizens' most intimate secrets with little oversight. However, the reality of the technological capability among police and national security agencies to thwart major crimes is practically unknown by Canadians.

The great challenge for the government and its security agencies, when they achieve these unprecedented powers, will be the shift from arguing for powers to operationalizing them in a timely fashion to keep Canadians safe.

A recently updated report by the Auditor General of Canada regarding the state of lawful information sharing between police from various jurisdictions in Canada suggests that we may be far from the advanced technological capabilities that Hollywood has dreamt up. The Auditor-General first reported in 2009 that the Canadian Police Information Centre Database (CPIC), a tool to share information on the criminal history of suspects and those who have been charged or convicted of new offenses, had a long lag time in being updated. In the update, it was reported that the backlog would not be fully up to date until 2018. Much of

[1] cbc.ca/news/politics/economy-not-terrorism-remains-canadians-top-vote-driver-1.2919792

the challenge pertains to the analog nature of many of the police agencies in Canada. It was further reported that some police forces sent paper copies of criminal records to have CPIC updated.[2]

At the heart of solving many modern security challenges, like basic information sharing, and the broader security-civil liberties dichotomy, is technology. Unfortunately, much of the global skepticism regarding government and law enforcement's respect for civil liberties is perceived to be technologically-driven.

The nature of national security and public safety threats continues to evolve quickly. Just as technology has enabled global commerce at rapid rates, crime has globalized and reached velocities never seen in history. The Internet has become a tool for terrorist recruiting and training, human trafficking, and child exploitation among other crimes. Recently, in a speech to the Council on Foreign Relations, the US Central Intelligence Agency's Director, John Brennan, stated that "the overall threat of terrorism is greatly amplified by today's interconnected world, where an incident in one corner of the globe can instantly spark a reaction thousands of miles away; and where a lone extremist can go online and learn how to carry out an attack without ever leaving home."[3]

A whole new category of crime, cybercrimes, has proliferated. According to a study by the Centre for Strategic and International Studies, the annual cost of cybercrime to the global economy is estimated at as much as $445 billion.[4] Law enforcement officers are saddled with the burden of dealing with these new types of crime and digital evidence while under resource constraints.

Beyond cybercrime and managing ever-changing forms of digital evidence, law enforcement is also faced with unprecedented jurisdictional challenges as it tries to protect citizens from the unscrupulous. A Council of Canadian Academies report, titled *Policing Canada in the 21st Century*, suggests that "the lack of coordination has the potential to become a much greater concern in the future given the growing cross-jurisdictional nature of crime."[5]

Law enforcement and national security agencies in Canada and around the world have the arduous task of understanding new technologies used by criminals, and developing and deploying their own technologies while balancing jurisdictional and civil liberties challenges. The technology industry has an important role in addressing these challenges.

The industry must be a partner of police and security agencies in managing technology and technological challenges. Governments, under the best of fiscal circumstances, cannot be expected to continually evolve to match the constant innovation of the technology sector. Details of these partnerships must be transparent to build trust with each other and the general public.

The technology sector, police, and national security organizations need to partner to develop new tools to not only address today's threats, but to also anticipate future threats. Such a partnership should put respect for civil liberties and managing jurisdictional challenges at the heart of its dialogue.

As governments work with these partners to practically address these challenges they should also aim to move the debate away from the dichotomy of security versus civil liberties. It should instead try to focus the public discourse on the nature of the threats we face, what technologies and subsequent legislative powers it needs to address them, and how the respect for civil liberties will be built in to the these systems.

One area that governments, working with law enforcement, national security agencies, and other partners may want to focus their attention in this regard is how to cross-analyse the data that has been lawfully acquired in cases across the country. Much of this data, from computers, smart phones, tablets, and other digital devices, sits idle awaiting trials or appeals, and upon the conclusion of legal proceedings goes into archives, often never to be thought of again. A utility that allowed for cross-case coordination, with parameters to respect privacy, could be an integral tool to unlocking evidence to prevent larger-scale crimes.

While the Hobbesian state of nature may never fully be eliminated, it is only through the purposeful co-development of tools that address the greatest security challenges of our time with an expressed purpose to respect civil liberties that we will see the technological lag between crime and law enforcement closed, and the supposed tension between security and civil liberties revealed as a false dichotomy.

---

[2] cbc.ca/news/politics/criminal-database-backlog-won-t-end-until-2018-rcmp-says-1.2991118

[2]cbc.ca/news/politics/criminal-database-backlog-won-t-end-until-2018-rcmp-says-1.2991118

[3] https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/director-brennan-speaks-at-the-council-on-foreign-relations.html

[4] csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

[5] www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/policing/policing_fullreporten.pdf

---

Neil Desai *is an executive with Magnet Forensics, a digital forensic software company in Waterloo, Ont. He also serves as a fellow with the Munk School of Global Affairs at the University of Toronto and the Canadian Defence and Foreign Affairs Institute. He previously served in senior roles with the Government of Canada.*