NATIONAL POST

Another fight over digital privacy is inevitable

Barry Cooper

March 31, 2016

Bill C-51, which is no longer a bill but a statute, the Anti-Terrorism Act, was controversial when introduced by the Canadian government last year. Its major feature expanded the remit of the Canadian Security and Intelligence Service and made it easier for government security agencies to share information. At the time, the third-place Liberals supported it, but during the election campaign they also promised amendments to create an all-party Parliamentary oversight committee similar in principle to those in the U.K. and Australia. (Full disclosure: I testified before a House of Commons committee looking at C-51 and recommended greater, but secret Parliamentary oversight.)

C-51 was widely seen as a response to the attacks on Oct. 20, 2014 by a home-grown jihadist terrorists on two Canadian Forces soldiers in St-Jean-sur-Richelieu, Que., and two days later on Parliament Hill. Despite the alarmist opinion that C-51 was aimed at such organizations as Greenpeace, it was clearly aimed at terrorists.

In short, the FBI sought to change the boundary where national security begins and digital security and individual privacy end.

Critics have also said that the Anti-Terrorism Act was an attack on the privacy of Canadians comparable to the legal battle in the U.S. between the Federal Bureau of Investigation and Apple Inc. that seems to have now been resolved with the U.S. government dropping the lawsuit. Apart from minor differences between the relevant Canadian and American laws, the real difference between what the Canadian government properly obtained in the Anti-Terrorism Act (amended or not) and what the American government was seeking to do is much more significant.

On the surface, the FBI simply wanted Apple to help unlock encrypted data stored on an iPhone that belonged to Syed Farook, an Islamic State of Iraq and the Levant-connected terrorist who murdered 14 people in an attack last December in San Bernardino, Calif. So, what's the problem? Despite the fact the suit was dropped, there are several important lessons for both Americans and Canadians.

To begin with, the FBI invoked the 277-year old All Writs Act. As the name implies, this broadly authorizes courts (the FBI says) to compel Apple to provide "reasonable technical assistance." Here things get tricky.

The iPhones' operating system — iOS – is encrypted and requires a pass code to unlock. It includes escalating delays for wrong guesses and, after 10 incorrect attempts, the data may be erased. So the FBI proposed that Apple provide a secret key, in the guise of an authentic, digitally signed software update, to bypass the security functions. This would enable the FBI to apply "brute force," trying all possible pass codes and eventually gain access to Farook's data. As one wag remarked, the government wanted to replace the iOS with FBiOS.

Apple responded by correctly arguing that requiring it to write and sign a fake software update would violate a First Amendment guarantee prohibiting government-compelled speech. The company also argued, and U.S. courts agreed, that an encryption algorithm is speech. The language happens to be computer code, not English or French, but it is still protected by U.S. law. Thus, just as the government cannot compel anyone to sign a petition, neither can it compel Apple to provide a signature to disguise spyware as a software update.

In short, the FBI sought to change the boundary where national security begins and digital security and individual privacy end. Only the agency's sudden announcement it had found another way to hack the phone prevented this case from going all the way to the U.S. Supreme Court.

This matters to Canadians for two reasons. First, because Apple is a global company, if the FBI had succeeded, the Mounties and CSIS would have been close behind. Second, and worse, the growing "Internet of things" provides an even greater opportunity for governments to insert spyware masquerading as legitimate updates into everything from laptop webcams to the GPS in your vehicle.

As Julian Sanchez of the Cato Institute observed, the real conflict is not about getting information from a dead terrorist's iPhone. It's between the culture of suspicion that informs high-tech surveillance and the trust necessary to sustain the "global software ecosystem." Users of that "ecosystem," including iPhone owners, would have reasonably distrusted Apple if it had lost in court to the FBI. Citizens of democracies anywhere need to have minimal confidence and trust that their government does not treat them as subversives.

The ability to insert spyware surreptitiously into web-connected devices is the issue involved in the FBI-Apple litigation. Like it or not, Canadians have a dog in that fight