DECRYPTING THE IPHONE - EVERYBODY'S GOT SOMETHING TO HIDE, EXCEPT ME AND MY MONKEY

Posted on March 10, 2016

Categories: Insights, Publications

What do a drug arrest in New York in June 2014 and the death of Mr. Farook, a mass murderer in San Bernadino, California in December 2015 have to do with the ability of Canadian users of Apple devices to keep their data private? These are the events that led the FBI to seek court orders to require Apple to assist it in gaining access to two iPhones seized in the execution of search warrants.If these efforts to effectively deputize Apple are successful, the ability to secure data on an iPhone or other iOS device may be ultimately be reduced for all users including those in Canada. While Apple is the current subject of these applications, the same principle could be applied to any communications or devices whose contents are encrypted.

At the root of the debate is the right of an ordinary citizen to secure information in a way that gives them the exclusive right to decide with whom they will share that information. Although perspectives on Edward Snowden's actions vary, one of the conclusions resulting from his disclosures is that where government agencies have the technical means to access private information, legal prohibitions and oversight of these agencies may be insufficient to protect ordinary citizens from having their private information collected and stored on a wholesale basis. Technological prohibitions on the other hand may offer some such protection, but those technological solutions are, as the recent California case indicates, under attack.

In both the California and New York cases one rationale the FBI advances to support its request is the need to access the phone to determine the identities of others with whom the phone owners were involved in their criminal enterprises. There is an argument made from time to time that only those with something to hide have any reason to be concerned if the government has access to their private data. Firstly, as The Beatles put it in 1968, "Everybody's Got Something to Hide, Except Me and My Monkey". Secondly, as Snowden put it, "arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." Whether we have nothing to hide or nothing to say, we should all care about privacy and free speech because they are essential to maintaining a free and democratic society.

The two US cases pose slightly different technical challenges. In the New York case, the phone seized from the accused was an iPhone 5c running iOS 7. Apple has the technical capability to bypass the password in iOS 7

and earlier versions. In the California case, the phone was also an iPhone 5c, but it was running iOS 9. This version of the operating system protects personal data from unauthorized access by protecting the data with an encryption key that is tied to the user's passcode, which Apple does not keep a copy of. On an *ex parte* (in the absence of Apple) motion by the Department of Justice, the court ordered Apple to assist the FBI by writing code that could be installed on the phone that would disable the auto delete function, permit the FBI to electronically submit passwords to the device for testing, and ensure that software on the phone would not introduce additional delay between multiple password attempts submitted to the device. Apple has moved to set aside the California order. The public debate associated with the California order ultimately led to the New York court issuing its order declining to force Apple to bypass the password, even though evidence disclosed that Apple had complied with such orders in the past. According to a Supreme Court of Canada decision in *R v Fearon*, Apple has also unlocked iPhones sent to it by Canadian authorities.

The issues these two cases raise are not black and white, but subtle shades of grey that are difficult to distinguish. For instance, in the California case where Apple is resisting the order to write the software requested by the FBI, it appears that some of the data on Mr. Farook's phone might have been more readily accessible had his employer not reset the password on his iCloud account at the FBI's request. Apparently Apple suggested a series of steps that it says would have resulted in portions of the data on the phone being backed up to iCloud where it could have been accessed by means of an appropriate warrant. The FBI have stated that "It is unknown whether an additional iCloud backup of the phone after that date — if one had been technically possible — would have yielded any data," What is clear is that the manner in which the password was actually changed did not create a more current iCloud backup.

The proper balance between protection of privacy and the protection of the public is difficult to achieve. While the Apple litigation in the US certainly flags many of the same issues that are applicable to Canadians, this litigation will resolve those issues in the context of US constitutional principles. If Apple is ultimately required to write the program it has been ordered to write in California, this will impact Canadian users because once the tool is available, there will undoubtedly be multiple agencies, including those in Canada, with cases they will say justify the use of that tool.

Under Canadian constitutional law, individuals have privacy rights with respect to matters over which they have a reasonable expectation of privacy. Where such an expectation exists, law enforcement requires specific authority to conduct a search (i.e. a warrant). In determining whether a reasonable expectation of privacy exists, a court will consider whether an individual has a subjective expectation of privacy and whether that expectation is objectively reasonable. The Supreme Court of Canada has recently recognized, in cases such as *R v Fearon* and *R v Cole*, that technological devices, such as computers and cell phones, attract a reasonable expectation of privacy in that they often contain a host of information revealing intimate details of one's private

life.

In many ways a modern cell phone or tablet is the embodiment of the telescreen George Orwell envisioned in "*1984*". It isn't just the e-mails you send and receive or the "selfies" that you take. Every request you make to Siri is forwarded to an Apple server, and processed there. At least for a period of time these data sets are also stored off the phone. If location services are enabled (and possibly even if they are not), your phone will diligently track everywhere you go. Connected devices like fitness trackers gather and store (and broadcast with varying degrees of security) all sorts of personal data.

Despite having a reasonable expectation of privacy, however, law enforcement still may be permitted to conduct searches of these devices upon gaining lawful authority to do so. As the California case makes clear, if you use iCloud (or another cloud storage service) to back up your device, it does not matter how secure a password you select on the device if all of your data is backed up on a remote server in a manner that is accessible by law enforcement upon obtaining an appropriate warrant.

Perhaps the more important lesson to take away from the US Apple litigation is that owners of these devices need to be much more aware of exactly what data they store as well as where and how they store it. Without understanding the extent of data that is collected, and the increasingly powerful tools that are available to collect and cull through it, it is impossible to have an informed public debate on when and how these tools should be employed.

by Peter Wells, Rohan Hill, Joanna Vatavu and Mitch Koczerginski

A Cautionary Note