ISN
ETH Zurich

6 November 2014

Cybersecurity: A New Regime on Government-Compromised Encryption

Do today's encryption standards represent a threat to cybersecurity, especially if they limit the intelligence gathering and law enforcement activities of government agencies? It's a question that Chris Bronk believes highlights the newfound power of the global IT industry, especially in the wake of Edward Snowden's revelations.

By Christopher Bronk for ISN

It appears that the encryption wars of the 1990s are returning to the policy agenda in the United States. This will likely impact global IT policy. In recent remarks, FBI Director James Comey made the case for U.S. law enforcement to gain additional capabilities to access data both at rest and in motion for the purposes of prosecuting criminal cases. This comes on the heels of announcements by Apple and Google that they are or will be providing enhanced encryption on their mobile phones and tablets. Furthermore, neither company plans to provide a backdoor to subvert on-device data encryption. This sets off a potential return to the 'Clipper Chip' debate of the 1990s in which the US government eventually relented on its effort to gain backdoor access on encryption technologies and implementations constructed by U.S. firms. More importantly, if the US government relents again, it may represent the power of the IT industry to begin setting global norms on cyber-security beyond the reach of government control.

Asserting privacy

This latest controversy in computing politics began with Apple's release of its new privacy policy. In it, Apple CEO Tim Cook made several points in differentiating how it does business versus the no-cost Internet platforms such as Google and Facebook, publicly calling out the well-known development that, "Users of Internet services began to realize that when an online service is free, you're not the customer. You're the product." Following the swipe at his two large neighbors, both of which happen to generate most of their revenue from advertising, Cook reserved especially blunt words for Apple's position on compliance with the US or any other government regarding backdoor access to the computers, phones, and other devices the company produces, stating:

I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will.

Although Apple has publicly stated that it will comply with legal instruments (principally subpoena

or national security letter in the US) in providing data from its cloud service, it will not unlock an encrypted iPhone for the purposes of law enforcement investigation and doesn't appear to be willing to develop code for its devices that would allow it or anyone else to do so. This is an incredibly important development and stands as perhaps the most important policy stance taken by any company in Silicon Valley since the Snowden revelations.

Silicon Valley has a lot to lose if public trust in its products and services collapses . If there was one constituency that was conspicuously horrified by the information leaked by Edward Snowden, it was U.S. firms in information technology (IT). Snowden's leaks presented damning evidence that the United States government desired backdoors in hardware and software, mirrored data traffic for bulk collection, and copied the proceeds of social networks.

The "Snowden Effect" has produced an enormous backlash against U.S.-headquartered companies selling hardware, software and services in international markets. Sales for U.S.-made computing hardware such as networking equipment and high-performance servers declined in international markets as buyers wondered if those machines were compromised to a similar degree as had been repeatedly alleged by Washington about Huawei . Many U.S. tech firms share a perception that they are still clawing themselves out of a significant crater due to the revelation of PRISM and other NSA programs.

From wiretapping to mass access

For this reason, Director Comey's remarks will not be well received in U.S. computing and information tech firms. Asking for additional powers of the sort enumerated in the 1994 Communications Assistance for Law Enforcement Act (CALEA) now appears badly timed and provides evidence that the FBI is out of touch with the U.S. tech industry and global advocates for privacy. While CALEA mandated that telecommunications firms provide easy access to their infrastructure for wiretapping activities, the FBI's want list now appears to include a mechanism to acquire any data it requires from any device to perform a criminal investigation.

Here is where this line of argument runs aground. The review of intelligence activities following the Snowden affair sought to ease concerns that data collection upon American citizens for the purposes of foreign intelligence would not be used as evidence in prosecution of criminal cases. Comey's speech, on "the impact of emerging technology on public safety," casts his agency as overwhelmed by the speed of innovation in digital communications.

While Comey laments the difficulty of intercepting communications, leaving his agents in the dark as criminals hop across cellular and wifi networks, he reserves special attention for the proliferation of encryption to personal devices, opining:

[I]f the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

This vilification of widespread implementation of encryption is an unfortunate statement of significant proportions, especially coming from the person who oversees what is by far the largest cyber-crime investigation organization in the US government.

It is a statement that seeks to undo what many in the field of cyber-security work toward: trying to

protect computers, networks, and the rapidly growing number of Internet Protocol devices springing up throughout homes and national infrastructure. The cybersecurity community wants better protections turned "on" by default, yet Comey is arguing that they should be turned "off" or removed altogether. This reveals the extent to which Director Comey is at odds with the cyber-security community and how little the concept must be understood within the Bureau.

Why no default encryption?

Cryptographic protections, the FBI argues, are powerful security tools for terror organizations and pedophilia networks that cannot be easily surmounted. While any rational and well member of society recognizes the threat of terrorism and child pornography, we must ask if the threat politics of these two issues requires the dismantling of cryptographic features that may prevent millions of devices from being vectors for identity theft, privacy violation, and other data crimes. The basic question here is whether the IT industry should surrender superior implementation of security to provide access to the investigative or intelligence organs of government.

In this latest round of the security/privacy debate, little has been mentioned regarding encryption software purveyor TrueCrypt and its demise. As we know, TrueCrypt died as a commercial entity, ostensibly because OS manufacturers gradually incorporated disk encryption features over time. However, there is a more conspiratorial narrative that TrueCrypt's undoing was its unwillingness to play ball in some way with the US government. Lavabit email service CEO Ladar Levinson claims that he was presented with such an ultimatum and chose to shut down his company rather than hand over the company's database of users' private encryption keys.

Countering the increasingly sophisticated encryption techniques employed by online pedophiles to shield themselves was cited by Comey as a significant concern.

The FBI and Silicon Valley appear to be gearing up for a battle over the FBI's desire for CALEA-like powers for software and device endpoints in mobile computing. One of the lessons of the Snowden episode has been that if the government doesn't get its back doors, it will be clever in tailoring access or defeating cryptographic implementation. Is it not fair for U.S.-based tech companies to make the argument that the US government continue on this path?

The United States government is creating a paradox: it is pushing for backdoor access to popular computing devices, social networking platforms, and the data transmission services (for which the term wiretap is now terribly out of date) while simultaneously calling for better cybersecurity for U.S. government agencies, corporations, and individual citizens. These, however, are not objectives that can be achieved in parallel. It cannot at the same time have Director Comey arguing for watered-down security and then have the FBI Cyber Division chief advocating for better cooperation between industry and government on security .

Dollars, euros, pounds, shillings and pence

For the global firms that comprise the IT industry, the requests for end-runs around default security features are not a favorable selling point in large and growing overseas markets. Apple's Q3 earnings report provides ample justification for resistance on meeting demands for weak on-device security from government, that of the United States or others. Roughly half of the company's revenue came from markets outside the Americas or Apple's retail arm, some $8 billion from Europe and more than $5 billion from China alone. Apple is making the bet that good privacy is good for business globally, which is something the U.S. Department of Justice doesn't seem to understand.

This clash on enhanced security and user privacy is a defining issue for IT. For companies that wish to be considered trustworthy on security, kowtowing to government may be becoming unacceptable. One industry employee from a very large US software firm opined at a conference recently that the United States government now falls within the category of Advanced Persistent Threat actors along with Russia and China. Such thinking represents a strong departure from the status quo. Not only are backdoors bad for security, but they also represent a potentially unaffordable cost to global firms and brands in IT. Furthermore, they will be bad for any tech firm wanting to do business in countries with robust data privacy laws or regulation, such as within the EU and a growing number of places elsewhere. Advocating for easily compromised encryption does nothing to help Washington get past the Snowden hangover.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources .

Christopher Bronk is the Baker Institute fellow in technology, society and public policy (TSPP) at Rice University. He previously served as a career diplomat with the United States Department of State on assignments both overseas and in Washington, D.C. He holds a Ph.D. from The Maxwell School of Syracuse University and studied international relations at Oxford University.

Publisher

International Relations and Security Network (ISN)

---

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?ots591=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=185017
