Why The Apple Versus FBI Debate Matters In A Globalized World

Mar 2, 2016 @ 03:47 PM

A man walks up the stairs at the Apple Store in Grand Central Station. (TIMOTHY A. CLARY/AFP/Getty Images)

Lost among all of the breathless headlines and hyperbole about the Apple versus FBI debate over the last few weeks is the global context in which this goliath versus goliath conflict is happening. Global companies like Apple build products that are sold all over the world, meaning that the FBI's demands not only risk Apple's credibility outside the US by portraying its products as surveillance devices of the US Government, but if successful will

also embolden repressive countries to demand the same capabilities, creating a race to the bottom in which American countries must produce backdoors into their products for every major government. Here's why this all matters.

A quick look at some of the quotes defining the debate shows the stakes the two sides attribute to the clash. Apple in particular has taken its case to the court of public opinion in an attempt to sway the FBI to retract its request. CEO Tim Cook lamented that "Apple is a uniquely American company ... It does not feel right to be on the opposite side of the government in a case centering on the freedoms and liberties that government is meant to protect." In its legal filing, Apple further argued "Nothing in federal law allows the courts, at the request of prosecutors, to coercively deputize Apple and other companies to serve as a permanent arm of the government's forensics lab."

While the FBI has repeatedly argued that they are requesting access only to a single phone, it is impossible to create a software toolkit of the kind requested that will operate only on a single iPhone. Since there is nothing unique about that particular phone, the software could be easily modified to operate on any iPhone. Put in simpler terms, the request is equivalent to asking a lock manufacturer to develop a master key that opens all of its locks to allow the government to open a particular door of interest. While the government might promise to destroy the key afterwards, the mere existence of a master key would likely cause the government to request the same key every time it has a door to open and would similarly embolden every other government to request the same key to open all of the doors they have an interest in. In short, there is no way to make a backdoor that works only for this single phone – the process of creating the backdoor establishes a blueprint and workflow for compromising all iPhones.

Indeed, after Apple noted "Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the

FBI wins this case," the Director of the FBI conceded that "police departments and district attorneys around the country were also seeking similar access to locked phones and encrypted conversations in ordinary criminal cases" and that a positive ruling "will be instructive for other courts."

Noting the open ended stakes, Apple went as far as to wonder aloud "Should the government be allowed to order us to create other capabilities for surveillance purposes, such as recording conversations or location tracking?" As Apple sees it, if the FBI is able to legally compel Apple to compromise one of its devices to allow its data to be downloaded, what would stop the FBI from issuing a similar order to require Apple to quietly enable the microphone or GPS tracking on a phone of interest? In fact, there is already precedent for this scenario - in 2001 the FBI ordered the manufacturer of a major vehicle communications system to quietly turn on the vehicle's built-in microphone in order to spy on the driver.

Apple is certainly under no illusion that their phones are absolutely uncrackable by a nation state – rather they don't want to be responsible for creating the backdoor themselves. In fact, it turns out that the US National Security Council already tasked US Government agencies this past fall with the very requirement of defeating the encryption and access protections of consumer devices. As the Snowden revelations demonstrate, the government's spymasters are more than capable of developing highly sophisticated technological workarounds themselves.

In fact, none other than Michael Hayden, former director of both the CIA and NSA, argued against the effort, stating "I think on balance that actually harms American safety and security, even though it might make [the FBI's] job a bit easier in some specific circumstances." In an interview with USA Today he noted "Look, I used to run the NSA, OK? Back doors are good. Please, please, Lord, put back doors in, because I and a whole bunch of other talented security services around the world — even though that back

door was not intended for me — that back door will make it easier for me to do what I want to do, which is to penetrate. But when you step back and look at the whole question of American security and safety writ large, we are a safer, more secure nation without back doors ... a lot of other people would take advantage of it." Indeed, the Juniper breach offers an abject lesson in how easily backdoors can be exploited by adversaries.

Critics have pointed to the fact that in just the first six months of 2015, Apple "received nearly 11,000 requests from government agencies around the world regarding information on roughly 60,000 devices ... [and] provided some data in roughly 7,100 of those requests." That makes for a 65% compliance rate. Yet, those requests involve data in Apple's cloud, which it acknowledges making available to law enforcement when presented with valid legal requests. In fact, that was one of the purposes of Apple creating a secure smartphone – that users could restrict highly sensitive data to the phone itself without uploading to the cloud.

Phones increasingly act as an extension of our bodies, recording our movements, health, purchases, searches, communications, calendars and even our most intimate thoughts. We carry our phones everywhere to the point they are increasingly being used as identification surrogates. What this means is that searching a phone is far more similar to the science fiction world of law enforcement being able to search one's mind than it is to rifling through the papers in one's living room.

Why does all of this matter? From 2013-2014 I was the Yahoo! Fellow in Residence of International Values, Communications Technology & the Global Internet at Georgetown University's Edmund A. Walsh School of Foreign Service, where I was also adjunct faculty. As the fellowship's name emphasizes, today's Internet is global and internationalized, meaning conflicts like the Apple vs FBI dispute play out in a globalized context.

In a globalized world, American companies do an ever-growing portion of their business abroad. In Apple's case, more than two-thirds of its revenue

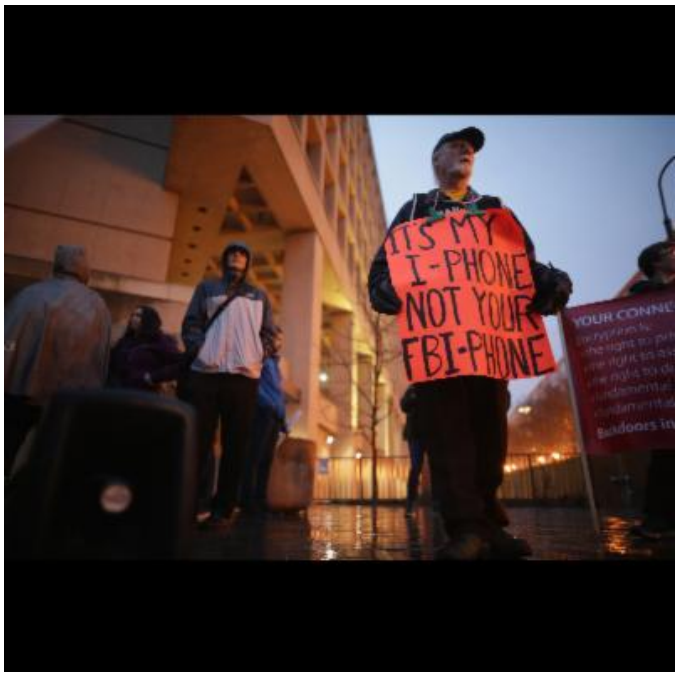
comes from outside the United States. It is not hard to imagine phone manufacturers outside the US touting their phones as being "backdoor free" and framing Apple's products as surveillance tools for the US Government, especially in light of the Snowden NSA disclosures. Imagine the reverse – a major Chinese consumer product manufacturer is ordered by the Chinese government to develop a backdoor providing it the ability to bypass device encryption and access controls. Similar to the overall encryption debate, the notion that creating a backdoor for the US Government will have no broader impact fails to recognize the globalized nature of commerce and the internet today.

Perhaps most profoundly concerning about the present conflict is that in this globalized world, if the FBI prevails, it is almost certain that every other nation will demand the same level of access. As former US Solicitor General Ted Olson grimly put it "The implications of this are quite serious … people in foreign countries are going to be very, very susceptible to invasions of their privacy if Apple can be forced to change its phone." In fact, just last year "Beijing backed off several proposals that would have mandated that foreign firms provide encryption keys for devices sold in China after heavy pressure from foreign trade groups. Nonetheless, a Chinese antiterrorism law passed in December required foreign firms to hand over technical information and to aid with decryption when the police demand it in terrorism-related cases."

As the New York Times put it, "China is watching the dispute closely. Analysts say that the Chinese government does take cues from the United States when it comes to encryption regulations, and that it would most likely demand that multinational companies provide accommodations similar to those in the United States. … China would also most likely push to acquire any technology that would allow it to unlock iPhones. Just after Apple introduced tougher encryption standards in 2014, Apple users in China were targeted by an attack that sought to obtain login information from iCloud users."

Just yesterday a Facebook executive was detained by Brazilian law enforcement after the company was unable to provide decrypted communications of an alleged drug dealer, showing the stakes involved for American companies as governments around the world eye the kinds of backdoor access demanded by the FBI.

In short, the Apple versus FBI debate is about more than just a single iPhone – it is about the limits of the US Government's powers to require American companies to custom engineer backdoors into their products that defeat consumer security and how those limits will affect the products and employees of American companies around the world. What the US Government succeeds in requiring, every other country will most certainly demand as well, subjecting American companies to the burden of creating backdoors for every government that requests them. In the end, as with the freedom of the Internet itself, privacy will fade away and the world's citizens will be only "as free as the world's least free place."



Gallery

Apple vs. The FBI: The iPhone Encryption Battle

Launch Gallery