The Implications of Creating an iPhone Backdoor

Gregory Coutros
American University Washington College of Law

Follow this and additional works at: https://digitalcommons.wcl.american.edu/nslb

Part of the National Security Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/nslb/vol6/iss2/5

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
THE IMPLICATIONS OF CREATING AN iPHONE BACKDOOR

GREGORY COUTROS*

The Federal Bureau of Investigation’s request that Apple provide an electronic backdoor into the iPhone left behind by one of the San Bernardino shooters is a reasonable, albeit difficult, request. It makes sense that the government would ask the company that created iOS to be the one to provide a backdoor into the device, as it is most readily able to do so. The government argued that accessing the phone was important to discover who the shooters had been working and communicating with in order to protect against the possibility of similar terror attacks. However, creating a backdoor into the iPhone sets a dangerous precedent and creates a powerful technological tool.

Destroying something once created in cyberspace is nearly impossible. The FBI argued that it was only requesting access to a single phone; the Bureau did not want nor expected Apple to create a backdoor to all iPhones. However, Apple pointed out a flaw in the FBI’s argument—because the process used to create the backdoor “could be replicated[,]” the code “would not be truly destroyed” even if Apple nominally did so after its intended use. Meaning, the code creating a backdoor could be reproduced and applied to other mobile devices. This would eliminate any security measure the original operating system had in place for any phone that uses the same operating system. The code used to create the backdoor would result in a skeleton key that could prove to be a major cyber security threat.

Because of the nature of the Intelligence world, the information on the phone could be more valuable than protecting against a potential cyber security threat against an aging Operating System. Gaining access to the iPhone would provide the Intelligence Community with names

---

* Gregory Coutros is a first year student at American University Washington College of Law, and a junior staff member on the AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF (NSLB). This brief article was originally published on the NSLB’s website as a blog post.

2 Davidson, supra note 2.
4 Chris Smith, An iPhone backdoor like the FBI wants is even more dangerous than you think, BOY GENIUS REPORT (Feb. 26, 2016), http://bgr.com/2016/02/26/apple-fbi-iphone-hack-backdoor/.
5 Smith, supra note 5.
6 Smith, supra note 5.
7 Smith, supra note 5.
8 Julian Sanchez, Apple vs. FBI: “Just This Once?”, JUST SECURITY (Feb. 23, 2016), https://www.justsecurity.org/29453/apple-vs-fbi-just-once (noting that while protecting a single private key is possible, protecting one that needs to change and adapt to every request to access different phones is nearly impossible).
and communications; from there, the possibility exists to discover other possible terrorist links. Additionally, should a precedent be set, whenever a phone or similar device is discovered, Apple would have a hard time arguing that the phone should not be unlocked. In the context of intelligence gathering, any information gathered by law enforcement could prove to be the one missing piece of a puzzle. Therefore, the faster a law enforcement agency is able to gain access to a device, the faster intelligence can be gathered and analyzed.

Information in the Intelligence Community is passed from agency to agency in a way that is designed to help piece together information and form a picture of what is happening. For instance, the “FBI can share information with . . . the CIA,” because one agency has information that the other needs. This flow of information can be used to help create a clearer picture of a potential threat. By gaining access to the content (rather than just the metadata) of the San Bernardino shooter’s phone, the FBI could potentially determine how the attack was orchestrated and who else was involved. With access to this valuable information, the FBI and other agencies could work to prevent the terrorist network involved with the shooting from carrying out another similar attack. Unfortunately, the FBI’s approach could set a dangerous precedent that affects privacy rights for the sake of only potentially stopping a threat.

This is a fight that has already started to play out in court. In the United States District Court for the Central District of California, Judge Pym ordered Apple to create new software to unlock the phone. However, in the United States District Court for the Eastern District of New York Judge Orenstein refused to require Apple to do the same with the phone of a drug dealer. Despite these conflicting rulings, it appears for now that the issue in the San Bernardino attack is on hold. The FBI recently requested to have the case dropped because the FBI discovered a way into the phone. The court approved their request.

Currently, there is a Manhattan prosecutor waiting to learn how the iPhone case will play out because he has 175 locked iPhones that are presently inaccessible. Although it appears as though that prosecutor’s efforts have been frustrated for the moment, the hypothetical persists—if a court finds that Apple is required to create this backdoor for the FBI, prosecutors around the

---

9 Sanchez, supra note 9.
10 Christina Sterbenz, Ex-FBI officials explain why the government wants Apple to provide access to the San Bernardino shooter’s iPhone, BUSINESS INSIDER (Feb. 22, 2016), http://www.businessinsider.com/what-ex-fbi-officials-think-about-apple-2016-2 (detailing how information gathered from different intelligence agencies is compiled and shared).
11 Sterbenz, supra note 11.
12 Sterbenz, supra note 11.
16 Chesney, supra note 4.
18 Ackerman, supra note 14.
country will begin to follow suit. Every prosecutor in the country who stumbles upon a cellphone in the possession of a suspect could request the contents of the phone be provided by citing to the Apple case.\textsuperscript{19} Even if there is no guarantee that the content on the phone is crucial to the case, the argument could be made that the intelligence value of the information will justify the request.

Creating a backdoor is dangerous.\textsuperscript{20} It creates a slippery slope, both technologically and legally. A legal precedent would be set that could make it easy to access the contents of a suspect’s phone, which would potentially alter privacy rights related to cellphones. In terms of technology, a skeleton key that could potentially be used to access anything that runs the same operating system would be created. No one would argue that trying to prevent another San Bernardino-type attack is not important, but is it important enough to allow for the creation of a skeleton key or a dangerous precedent? No, it is not. In the current interconnected landscape of society, the modicum of privacy that still exists is vital. To remove another safeguard could be disastrous.

\textsuperscript{19} See Ackerman, \textit{supra} note 14 (relating FBI Director James Comey’s acknowledgment that prosecutors and police departments around the country are seeking similar access to locked phones).