blogs.lse.ac.uk
http://blogs.lse.ac.uk/usappblog/2016/02/20/the-fbis-demands-to-hack-tashfeen-maliks-iphone-are-a-threat-to-everyones-online-security/

The FBI's demands to hack Tashfeen Malik's iPhone are a threat to everyone's online security.

The FBI says they want to see the contents of one mass murderer's iPhone. They are bringing the case, though, in the hopes that it will set in motion legal and political changes that would further reduce all Americans' right to privacy against government searches. **Bill Herman** *argues that the potential impact of that precedent, plus the resulting threats to everyone's online security, means we should all be concerned.*

On Tuesday, a federal judge in Los Angeles ordered Apple to help the FBI hack into the iPhone of the late Syed Rizwan Farook, one of the San Bernardino shooters. The contents of the phone are encrypted, and the FBI only gets ten wrong guesses at the password before the phone's security features erase all of the contents. If Apple were to write a custom version of the phone's iOS software, however, they could reboot the phone, load the custom software, and then allow the FBI to make an unlimited number of guesses, at lightning speed, until they get the right answer.

The court invoked a vaguely worded statute from 1789 to order a private sector technology firm to create a smartphone hacking tool that does not exist. Such a court order is totally unprecedented, and Apple is pushing back, hard.

The FBI clearly has bigger plans in mind. The agency must have hundreds of other encrypted iPhones in their evidence lockers that belonged to living suspects — suspects whose convictions would, in most cases, probably make a more meaningful contribution to public safety. After all, Farook and his wife, Tashfeen Malik, were killed in the attack, and the FBI quickly concluded that the couple most likely acted alone. Yet the feds waited for this case to try out this specific legal theory. This is not a coincidence.

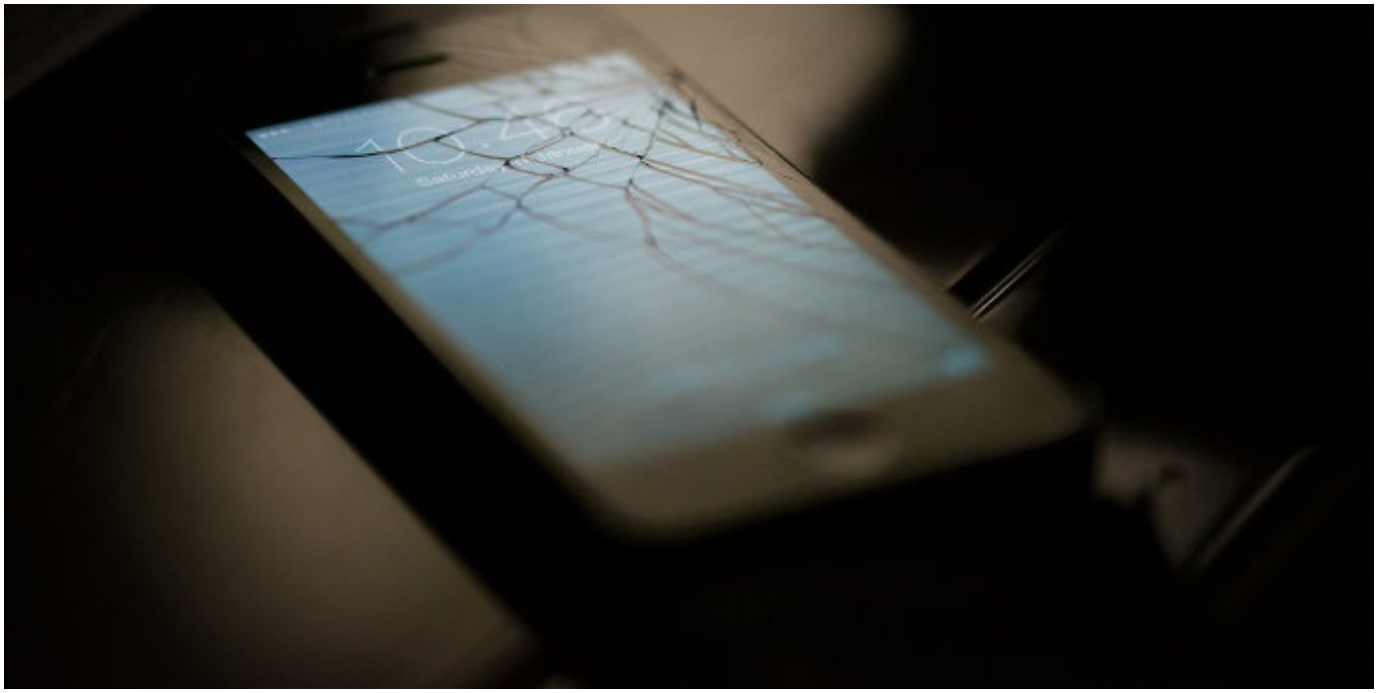
This has every appearance of being an act of impact litigation, or the pursuit of a specific legal precedent that will shape broader policy for many more people than those with a stake in a given case. This usually means nonprofits such as the ACLU and NAACP arguing cases featuring highly sympathetic people who can stand in for the interests of a large group of people. Here, the FBI wants to undercut the rights of everyone, so they're using an especially despicable person as a courtroom exemplar.

According the *New York Times*, "Law enforcement officials who support the FBI's position said that the impasse with Apple provided an ideal test case to move from an abstract debate over the balance between national security and privacy to a concrete one." Not just any concrete case, though — one involving perhaps the most despised criminal suspects of the decade.

The law enforcement community wants to effectively end your ability to use strong encryption, and they're waging this war in the courts and on Capitol Hill. FBI Director James Comey went to Congress last July, and again in December, to push for legislation that would require tech companies to build their devices so that law enforcement would have special backdoor access. Even barring legislation, the national security community is making a sustained push to defeat encryption on network connections and devices.

This push continues even though top cryptologists are unified in their opposition to the plan. They argue, in one unified voice, that it is not technically feasible to enable special government access and *not* create additional vulnerabilities to hackers and foreign governments. Further, in a post-Snowden world, we should also be worried

about security against secret government intrusion.



Credit: Faris Algosaibi (Flickr, CC-BY-2.0)

The terrorists, kidnappers, and child pornographers are just the boogeymen here. If Apple loses, the new tool can and will be deployed against garden-variety criminal defendants. While terrorism has a special place in our political discourse, it is not special in terms of the rules that courts use to govern the collection and admission of evidence. The same rules will then apply to crimes as pedestrian as mail fraud and trafficking marijuana. Also, once Apple does it for the FBI, every state and local jurisdiction that can't crack an iPhone will go to court to demand the same kind of access. They will probably get it, too; that's how US legal precedent works. Foreign governments will also all start demanding access to enforce their own laws.

Once the precedent exists for an iPhone in the state's possession, it is a small (legal) step to order Apple to do the same thing for remote surveillance. (I am no engineer, but it seems quite feasible to put this code into a new OS update that gets pushed out remotely.) Imagine your phone being compromised without it ever leaving your possession.

Now imagine every law enforcement agency in the country being just one local judge's court order away from having that kind of access to the intimate details of your life. Our federal, state, and local law enforcement is conducted in a highly discriminatory fashion. Comey himself had to help clean up when the FBI railroaded innocent defendants toward prison. If you think you have nothing to hide or that it couldn't happen to you, you're mistaken. As Aleksandr Solzhenitsyn observes, "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is." Are you confident that the police won't take an interest in you? Don't be; all it takes is one traffic stop.

This issue will only become more salient as our homes increasingly become internet-connected smart homes. The police would love to be able to turn any smart TV or home thermostat into a surveillance device. As world-renowned digital security researcher Bruce Schneier points out in his excellent book *Data and Goliath*, surveillance used to be expensive and thus rare. Now that it is cheap and easy, government surveillance has exploded. If the FBI wins this case, we may be headed for a future of the state regularly turning all of the internet-connected cameras and microphones in our homes against us. Many of the warrant requests will even go through the secretive and highly

compliant Foreign Intelligence Surveillance Court.

Even if you aren't worried about government surveillance, though, you should be worried about the explosion of security vulnerabilities this would represent. Apple, the world's most valuable company, has one of the finest collections of engineering talent ever assembled. Yet even Apple's own corporate computers have been compromised, showing that no company is safe. If each company must keep a set of master keys on its servers, many of these master keys will be purloined by hackers — and oppressive foreign governments. The problem will be exponentially worse for smaller and less security-obsessed companies, who still make up a substantial part of the digital equipment economy.

The problem is made even worse if this precedent is set and then, in this or a future case, combined with the rules of forensic evidence. As one forensics expert explains, Apple is being ordered to create a forensic instrument, and these are subject to detailed review by third-party analysts, including experts hired by defense attorneys. This would create a secret of explosive value being entrusted not merely to the FBI, but a large number of people with widely varying security procedures and incentives to keep the secret. Any skilled attacker would need only to find and penetrate an attorney's IT system (many of which are ordinary home routers) and walk away with the keys to hundreds of millions of devices. The identities of those who possess this secret will become a matter of public record. Apple may have to disclose critical details in open court. The iPhone is the most valuable consumer device in the world, and a tool to hack it would give the possessor the capacity to learn more secrets about more people than any mid-century police state could have imagined.

If the FBI wins, in court or in the legislature, then it is almost inevitable that vastly more people will have their identities stolen; that more will see their intimate personal content leaked online; and that, in oppressive countries, more will be punished for political or religious expression. Our collective security will be harmed, not helped.

The FBI didn't choose this case by accident. They want to be able to hack into anybody's inner digital sanctum, as quickly and cheaply as possible — consequences be damned. They chose this case because "terrorism" is the rhetorical talisman that turns off our ability to think rationally about what we stand to lose. In this case, we stand to lose a lot, starting with our ability to trust the updates on any of our internet-connected devices.

In short, it's not really about Syed Farook's cell phone at all. It's about yours.

Please read our comments policy before commenting.

Note: This article gives the views of the author, and not the position of USAPP– American Politics and Policy, nor of the London School of Economics.

Shortened URL for this post: **http://bit.ly/1PPhDwb**

About the author

Bill Herman – *Fordham University*
Bill D. Herman is an Assistant Professor of Communication and Media Management at the Gabelli School of Business at Fordham University. His research and teaching interests live at the intersection of communication technologies, policy, politics, and media industries.