Institute for Communitarian Policy Studies

I often write about rather different matters, but in my mind they all deal with one core question: the guidance our shared values, especially the common good, provides to our public policies.

"Hi Techies" Feedback, Advice for Activists

March 18, 2016

Copyright: Stuart Maxwell, Flickr Creative Commons

An Apple—FBI compromise?

I asked a list of colleagues the following (their responses follow, all quoted with permission):

Please let me know if in the following way we can have our Apple and eat it too. Seriously—allow the FBI to get the information protecting national security requires—and protect the privacy of other phone users. Apple argues that if it introduced a backdoor into the high power encryption program it inserted into its new phones, this vulnerability would allow foreign governments, criminals, and hackers to violate the privacy of many millions of phone

users around the world.

Let us assume that Apple leaves the phones as they are—but develops a key to unlock them it keeps, protecting it by using Apple's high power encryption. Once a court orders that a given phone must be unlocked, the FBI will bring it to Apple, which will unlock it, and turn over to the FBI the found information —but not the key. (NY Police Department alone has 300 such phones waiting to be "read')

What is wrong with this approach?

Granted, applying the same methods to phones that is still in the hands of terrorists, drug lords, and human traffickers, raises additional challenges. But here too, as long as the surveillance is carried out via Apple—the encryption of all other phones is not threatened.

Apple argues that if it did so for the USA—other governments would demand the same access. If Apple feels it cannot resist such demands, what is to prevent China and Russia from demanding access even if US did not get it?

Apple sometimes says that it cannot unlock these phones, but it told the court that this would be expensive—i.e. it can be done. Moreover, the Wall Street Journal pointed out that it would cost merely the same as one engineer for one year.

There are many other reasons Apple and other high-tech corporations give for objecting to collaborating with the government.

I am asking merely a technical question. Can a key kept by Apple under its high power encryption unlock selected phones without making other phones vulnerable?

Kindly respond to etzioni@gwu.edu and also let me know if I may quote you. For more about this topic, see my paper on "Ultimate Encryption" on SSRN.

James H. Morris, Professor of Computer Science, Carnegie Mellon

What you suggest is certainly possible. In fact, what the government is asking--that Apple install an operating system that will allow the FBI to try millions of passwords--has the same proproperty: only Apple could repeat it. There's no back door here.

Furthermore, it would probably cost Apple 5 minutes on an engineer's time, simply commenting out the code that bricks the phone after ten rapid password guess.

I think this is entirely a battle over the legal precedent. Apple knows, it submits now, it will be very hard to refuse in the future, even for China or Russia.

Also, the government is after a precedent and chose this case carefully to maximize the public support for their case. They could have chose any of the 300 other cases, but they

weren't about terrorism.

Steve Bellovin, Professor, Dept. of Computer Science, Columbia University

You asked “I am asking merely a technical question. Can a key kept by Apple under its high power encryption unlock selected phones without making other phones vulnerable?”

The short answer is "no".

For full details, seehttp://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009 (I'm one of the authors) and Susan Landau's Judiciary Committee testimony athttp://judiciary.house.gov/_cache/files/b3af6e9e-b599-4216-b2f9-1aee6a1d90cd/landau-written-testimony.pdf. Briefly, there are several different problems. First, what you suggest -- encrypting under a key known only to Apple -- sound easy but isn't. Cryptography is a very subtle technical discipline; it's very hard to get even the simplest things right. To give one example, see https://www.cert.org/historical/advisories/CA-2000-18.cfm? -- an "additional key" solution that turned out to be fatally flawed in a fashion that is blindingly obvious after the fact. Nevertheless, the mistake occurred in product from a company whose business was selling cryptographic solutions, i.e., one that you'd think had the competence to avoid such errors.

Second, with the thousands of phones that need to be unlocked in the US alone (if Manhattan alone has 200 and (per an article I read last week) Sacramento County has 80, the nationwide number can't be less than that), protecting this one Apple key and/or its use becomes very difficult. (See Landau's discussion of "routinization".) A key can be readily available or it can be secure; it can't be both.

Third, the existence of this key is a magnet for nasty governments. Maybe Apple is good at resisting ordinary hackers, though they're a sufficiently secretive company that I don't know if we'd know if they were hacked. For that matter, I don't know if they'd know; most victims never notice. (Home Depot found out they'd been penetrated for 6 months not by their own technical efforts but because some banks tracked a pattern of credit card fraud to their customers.) Intelligence agencies, though, are way ahead of ordinary hackers. China hacked Google 6 years ago, and Google is acknowledged to be one of the best in the business.

By the way, you wrote "protecting it by using Apple's high power encryption". That's the wrong approach; that just moves the problem to protecting another key. For this, you need technical, physical, and procedural security measures, probably not more encryption.

John Pike, Director, GlobalSecurity.org

Let us assume that Apple leaves the phones as they are but develops a key to unlock them it keeps, protecting it by using Apple's high power encryption. Once a court orders that a given phone must be unlocked, the FBI will bring it to Apple, which will unlock it, and turn

over to the FBI the found information but not the key.

I have tried not to follow this controversy, since so many other people are following it. But I think that this is what is being proposed.

As long as the surveillance is carried out via Applethe encryption of all other phones is not threatened.

I think that Apple is arguing that they cannot protect the security of their gizmo, which would find its way out of Apple and into the hands of evil-doers.

China and Russia from demanding access

That is, how can Apple resist lawful orders from unsavory governments. Their argument is that the existence of such governments means that no government anywhere can enforce a lawful search warrant. I try to avoid pretending to be a lawyer, but this would seem to make compliance with any search warrant a voluntary affair, or at least allow the subject of the warrant to condition compliance with their assessment of the legitimacy of the issuing authority.

Can a key kept by Apple under its high power encryption unlock selected phones without making other phones vulnerable?

Again, their claim is that the dang thing would escape their premises, and get into the hands of evildoers.

David Bantz, Chief Information Architect, University of Alaska system

Of course Apple could create and selectively apply a version of their OS to phones identified by law. That is pretty much exactly what they've been asked to do by FBI.

But once you have a special version of the OS that disables protections against guessing password to unlock the phone, how to prevent it from getting abused - for example to unlock your phone or mine? NYC and FBI have hundreds of phones they want to unlock.

That would entail a process involving many people and loading the OS on many phones. That makes it possible maybe even likely that one of those people entrusted with that power is coerced or bribed or is clumsy enough to put it in the hands of criminals.

At that point the criminals can unlock your phone and mine. They could then read your documents, install their own software to steal your passwords or track your use.

Maybe you trust that even with hundreds of agents and Apple employees use the broke OS on hundreds or thousands of phones their performance will be perfect so that no criminal gets he broken OS. Do you trust that enough that you would very sensitive info to that process? Many will not, and that lack of confidence means we have lost confidence in the

security of our info and opened ourselves up to invasive intrusion via malware installed without our knowledge.

(The even more valuable thing to steal would be the secret key that has to be used to sign the OS so that your phone will accept the OS. With that a criminal can write their own even nastier more broken OS and push it onto your phone. The possibilities are endless.)

Amitai Etzioni:

Dear colleague,

I hear you but do you believe that means the FBI will be blinded? Or do you believe they are bluffing or there are not major costs if they are blinded?

Best, Amitai

David Bantz:

If you mean by “blinded” that the FBI won’t be able to break into an arbitrary iPhone by getting Apple to break the phone by pushing the OS that disables the phone’s security, then yes, they won’t be able to. In this particular case, apparently the FBI would have been in a better position to get information off the phone if they had not first reset the phone’s password (I don’t understand the details of that, but I’ve read semi-technical articles that assert so).

While I would like law enforcement to get information that help gets bad guys, the cost for some ways of getting information may be too high.

Stories about this Apple/FBI conflict usually state the issue in terms of privacy - that if the tool were to escape or be misused, individuals’ privacy could be violated. While that’s true, said that way it seems the trade-off is possible embarrassment - uncovering a person’s unwise email messages, or their viewing of smut. And since those seem venial and even uninteresting, it might seem little is given up (particularly since I bet we all think it’s someone else who will be embarrassed - not us).

But security is at stake too: the security of information that is rightly - necessarily - kept secret by law abiding individuals. Financial data is an example: your credit card numbers (with the billing and pin we regularly provide in buying books or socks on line), bank account passwords, and the like. While I can’t really imagine serious bad guys going to a lot of trouble to find your or my browsing history or read our emails, it certainly is worth their trouble to capture that financial data and max out our credit cards, get new cards issued in your or my name issued to them, transfer funds from our accounts and so on (I mean of course not one or two, but at scale). If you knew this was possible after many Apple employees had access to broken OS and the means to force that OS onto an iPhone (signing keys that would also work to force a different OS broken in other ways onto phones), would you still trust your financial secrets to be on that iPhone? And of course,

even if compromising my words and yours doesn't rise to a serious loss of security broadly speaking, compromising the email and documents of the government officials or CEOs surely would.

Here's a sounder slightly more technical account by information security maven Jeff Schiller: https://jis.gyv.name/home/pages/20160226

Jeffrey A. Eisenach, Senior Vice President and Co-Chair of NERA's Communications, Media, and Internet Practice

Actually, no..... not according to Apple. The govt has already offered the "you keep it" option -- indeed, not just keep it, but destroy it. Apple argues that simply the act of hacking the phone makes it more likely they will be asked to do so in the future.... Not a very credible argument I think.

Prof. Roger Bohn, Associate Dean, School of Global Policy and Strategy, UC San Diego

A quick response. Of course nobody knows all the answers in detail to your questions.

First, read up on what a "key" really is in this case. It's not at all analogous to a physical key.

Second, Apple's real concern is clearly not this case, but the precedent. The USG, in various cases elsewhere, as well as various states, have already made it clear that they plan to use a favorable judicial decision in this case for multiple other phones. So Apple, quite correctly, does not view this as a "one time" thing; it is setting a precedent. And it fundamentally does not trust the USG or any other government to act legally and with restraint.

Third, Anything can be reverse engineered. Once Apple creates this tool, and the source code that goes with it, there are numerous ways that other players can end up getting their hands on the core ideas, and implementing their own versions. It's like building the first A-bomb. It's still very hard to build another one, but look at all the security there, and USSR had its own within a few years.

Regarding other countries: You can answer this one yourself. Consider the difference in telling the Chinese government "No" in two scenarios.

1) "We did not do it for our own government, and we won't do it for anyone. That protects everyone who uses Apple products, including Chinese, from American espionage."

2) "We don't like you as much as we like the USG, so although we did it for them, we won't do it for you."

Which position is going to cost less for Apple to maintain, in the face of determined

pushback from Chinese government?

Andrew Percy, FRSA, CEO, Justworks, Silicon Valley, and Spokesperson for the LIFE movement

A single key to unlock all doors would be the greatest prize for the devil... and impossible to protect.

The answer is to set up the infrastructure that allows everyone to have their own key, but provide a mechanism to access to an individual's key with a court order.

This system is specified at www.Standardsoflife.org/xID.

Alexandr Burilkov, Research Fellow/Doctoral Student, GIGA Institute of Asian Studies

I'm not strictly speaking a techie, rather a political science grad student, but I work with statistics and programming and have some knowledge of cryptography.

Apple uses the same 256 bit AES standard encryption developed by the US gov't in 2001 and now in use across NATO and the private sector worldwide. The key is fused into the device at the hardware level, and with a decent password, a brute force attack that looks at all possible password combinations would take years on average to succeed.

What the US government wants is to have access to Apple's records of keys built into its devices. This can easily be done on a case-by-case basis, when a single device is brought to the court and decrypted by Apple. So yes, decrypting selected phones can easily be done without compromising others; if that weren't the case, the AES standard would be far worse than what it is, and wouldn't be in use by NATO.

As to the argument that China and Russia would demand access, I know for sure that at least the Russians have a very advanced surveillance network (SORM, active since 1995) analogous and perhaps even superior to the NSA. The Russians would likely much prefer to find a way to decrypt Apple devices that Apple isn't even aware of, rather than trying to pressure Apple openly, as the Chinese have done with Google. This would be possible when an user uses their Apple device and the signal carrying passwords and other sensitive information is captured by the Russians (here in Germany there was a similar scandal, when iPhones were hacked by thieves by capturing the signal in order to extract logins and credit card information).

Furthermore, in extremis the Russians would probably resort to coercion of individuals, and most encryption doesn't survive rubber hose cryptanalysis. Therefore, Apple's argument on that is rather spurious.

Clay G. Wescott, President, International Public Management Network

In my view, this isn't a tech issue, but a governance one. Countries like China routinely ask tech companies for information about dissidents, and the consequences can be long prison terms. Apple wants to be able to say no.

Philip A. Schrodt, Senior Research Scientist, Parus Analytical Systems LLC

This is in the current issue of Science and is a great example of how a system (BitCoin) that everyone wanted to be secure (even if some of the "everyone" were some nasty characters...) but through just a few people being a little sloppy, got compromised and once compromised (in this case by law enforcement), provides far more information than would have been available had the "secure" system not been used in the first place. Again, the problem is not the technology, it is people getting careless about how they use the technology.

Michael Boylan, Professor of Philosophy, Marymount University

I agree with you about having Apple unlock the phone under its own authority, keeping the phone in their care, custody and control, and turning over the files/information that would be mentioned in a court order. Apple would be safe. Foreign governments would only have leverage over Apple if they used economic arguments. For example, China could say, unlock this phone or we don't let you do business in China. Of course, in the language of statistics, this is an independent event. China might say this whether or not Apple acted in the U.S. case at hand. The two sorts of cases demand different sorts of internal standards on the part of Apple. I remember when Google pulled out of the Chinese market because it did not want to be a party to e-mail surveillance. Apple might choose to do the same--even though they (Apple) has manufacturing relationships as well with China (which do not adequately recognize employee rights). It is very interesting which "values" seem dominant within one's shared community worldview.

Bill Loughrey, former technology executive on two presidential commissions on encryption

This is about a simple thing called security. Would you live in a house if the terrorists had the key to it? Terrorists are tough guys. Do you think they will use technology or live in a house if the police have a key to it? Would you claim a product is secure if the law enforcement officials have the key to it? We used to have security built into the public infrastructure so that there was public access. It is now basically in the ends of the network where the technology companies control it. They don't build good security into their products, because they can charge more for it later on. Apple has totally blown it by letting their security be a public spectacle. They now have for less security than their had before. By the way, the terrorists are already using another technology - at least for their secure communications.

Brian Forst, PhD, Professor of Justice, Law and Criminology, School of Public Affairs, American University

Thank you for your thoughtful, concise assessment of the Apple vs US controversy. I think your question, "Can a key kept by Apple under its high power encryption unlock selected phones without making other phones vulnerable?" really extracts the essential question from the considerable clouds of smoke that this case has generated. I think the answer to this question can be summarized in terms of the slippery slope problem: Yes they could, but if they break precedent in this case there will be no end of other requests, and they can claim moral high ground by standing on the side of their customers' rights to privacy to avoid the hassle and build goodwill among their mostly liberal, educated customer base. That may sound cynical, but I've yet to see another explanation that makes more sense.

Vladimir Baranovsky, Russian Academy of Sciences, Centre for Situation Analysis, director

To 'a technical question: Can a key kept by Apple under its high power encryption unlock selected phones without making other phones vulnerable?' there is a strictly technical answer: yes it can! But the problem is by no means a strictly technical one. In so far as there is no 100 (hundred) per cent certitude that unlocking phones is technically impossible, - such unlocking becomes possible due to *human* factor.

Amitai Etzioni

Many thanks. While I am studying the various documents and reflect on what I learned, here are my thoughts on one key point: The argument that if Apple will help the US government it will have to do the same for other, authoritarian governments. From all these well-taken responses, there follows:

Apple's Chinese Red Herrings
Far from yielding to the FBI's call to help it gain access to messages stored in a terrorist's cell phone, Apple is doubling down: Apple is working to increase its iCloud encryption, which would inhibit even Apple itself from retrieving password-protected customer data stored in its cloud.

Congress must act soon to stop Apple
If Congress does not act soon to rule that the CALEA act applies to extremely strong encryption inserted into Apple phones, every terrorist, drug dealer, and human trafficker with half a brain will get one. They may have waited a bit to find out if these phones are really as impenetrable as both the FBI and Apple claim, but one must assume they are increasingly convinced

Join the conversation on Twitter using #bitetheApple.

Our Most Recent Tape

"Five Lessons for Activists"

Follow the Institute for Communitarian Policy Studies on Twitter, Facebook, or YouTube.
To subscribe to our other updates, send an email to icps@gwu.edu listing your fields of interest.

The Institute for Communitarian Policy Studies
Executive Associate in University Professors Department
1922 F Street NW, Room 413
Washington, DC 20052

(202) 994-8190