Connecticut Debate Association
March 7, 2015
Darien High School, Guilford High School and Pomperaug High School

Resolved: Technology companies should fully encrypt their products.

Apple and Others Encrypt Phones, Fueling Government Standoff

By DEVLIN BARRETT, DANNY YADRON and DAISUKE WAKABAYASHI, Nov. 18, 2014 10:30 p.m. ET, The Wall Street Journal

U.S. Says New Technology Will Hinder Police Investigations

The No. 2 official at the Justice Department delivered a blunt message last month to Apple Inc. executives: New encryption technology that renders locked iPhones impervious to law enforcement would lead to tragedy. A child would die, he said, because police wouldn't be able to scour a suspect's phone, according to people who attended the meeting.

At issue is new technology that Apple, Google Inc. and others have put in place recently to make their devices more secure. The companies say their aim is to satisfy consumer demands to protect private data.

But law-enforcement officials see it as a move in the wrong direction. The new encryption will make it much harder for the police, even with a court order, to look into a phone for messages, photos, appointments or contact lists, they say. Even Apple itself, if served with a court order, won't have the key to decipher information encrypted on its iPhones.

The meeting last month ended in a standoff. Apple executives thought the dead-child scenario was inflammatory. They told the government officials law enforcement could obtain the same kind of information elsewhere, including from operators of telecommunications networks and from backup computers and other phones, according to the people who attended.

Technology companies are pushing back more against government requests for cooperation and beefing up their use of encryption. On Tuesday, WhatsApp, the popular messaging service owned by Facebook Inc., said it is now encrypting texts sent from one Android phone to another, and it won't be able to decrypt the contents for law enforcement.

AT&T Inc. on Monday challenged the legal framework investigators have long used to collect call logs and location information about suspects.

In a filing to a federal appeals court in Atlanta, AT&T said it receives an "enormous volume" of government requests for information about customers, and argued Supreme Court decisions from the 1970s "apply poorly" to modern communications. The company urged the courts to provide new, clear rules on what data the government can take without a probable cause warrant.

Relations between the federal government and Silicon Valley have soured since revelations about government surveillance by National Security Agency leaker Edward Snowden —and the criticism of some technology companies that followed.

The new security measures threaten to alter the government's post 9/11 efforts to intercept terrorists and other suspected law breakers. Last month, Federal Bureau of Investigation Director James Comey said new Apple and Google encryption schemes would "allow people to place themselves beyond the law."

Robert Hannigan, the head of GCHQ, Britain's version of the NSA, wrote in the Financial Times earlier this month that U.S. technology companies "have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us."

As recently as 2012, Google Executive Chairman Eric Schmidt was on a first-name basis with then-NSA head Keith Alexander, published emails indicate. He and other Google executives participated in classified cybersecurity briefings on hacking threats facing the U.S.

In March, Mr. Schmidt declined a personal request by President Barack Obama for technical staffers from Google and the government to discuss what the NSA does and doesn't do, according to two people familiar with the exchange.

At a public hearing in October, Mr. Schmidt said NSA snooping would wind up "breaking the Internet."

Tech companies say concerns that they too easily turn over data to the U.S. government are costing them business overseas.

The dispute resembles the so-called Cypto Wars of the early 1990s, when the Clinton Administration sought to regulate certain encryption schemes like weapons and require that they include a key that could be unlocked by law enforcement. Tech firms resisted, arguing that people should be able to encrypt their information to safeguard it.

A federal appeals court mostly ended the dispute in 1999, when it ruled computer code, including encryption schemes, is protected speech under the First Amendment.

Over time, Washington and Silicon Valley repaired relations. Tech companies generally responded to government requests for data following the 9/11 attacks.

Then came Mr. Snowden's revelations, beginning in June 2013. The former NSA contractor released documents showing the NSA scanned Internet traffic extensively, suggesting tech companies were complicit in the snooping. Other documents revealed that the NSA had intercepted traffic between Google's overseas data centers, infuriating Google executives.

In June 2013, Mr. Snowden provided reporters with documents describing a government program called Prism, which gathered huge amounts of data from tech companies. At first, tech-company executives said they hadn't previously heard of Prism and denied participating. In fact, Prism was an NSA code word for data collection authorized by the Foreign Intelligence Surveillance Court. Tech companies routinely complied with such requests.

More than a year later, tech executives say consumers still mistrust them, and they need to take steps to demonstrate their independence from the government.

Customer trust is a big issue at Apple. The company generates 62% of its revenue outside the U.S., where it says encryption is even more important to customers concerned about snooping by their governments.

These days, Apple Chief Executive Tim Cook stresses the company's distance from the government.

"Look, if law enforcement wants something, they should go to the user and get it," he said at The Wall Street Journal's global technology conference in October. "It's not for me to do that."

In early September, Apple said the encryption on its latest iPhone software would prevent anyone other than the user from accessing user data stored on the phone when it is locked. Until then, Apple had helped police agencies—with a warrant—pull data off a phone. The process wasn't quick. Investigators had to send the device to Apple's Cupertino, Calif., headquarters, and backlogs occurred.

Apple has long encrypted customer communications through its iMessage and FaceTime services, introduced early this decade. That decision prompted separate complaints from law enforcement.

Shortly after Apple's announcement, Google said it had adopted a similar encryption scheme on phones using the newest version of its Android operating system, which was released in October.

The announcements set off alarm bells at the FBI, the Justice Department, and other law-enforcement agencies. Officials feared that other companies would follow suit, making even more communications paths difficult to investigate.

Since the Snowden revelations, Google, Facebook Inc. and Yahoo Inc. had begun scrambling information transmitted between their overseas data centers to block NSA spies from listening in. Microsoft Corp. fought a government request for information about users of its Ireland data center, arguing the government had no jurisdiction outside the U.S.

Twitter Inc. this fall sued the government, arguing a recent settlement between the Justice Department and other tech firms restricts what it can say about government data requests.

Soon after Apple's announcement, the FBI requested a meeting. The task of speaking for the government at the Oct. 1 meeting fell to Deputy Attorney General James Cole, the Justice Department's second-ranking official. Mr. Cole had previously brokered the settlement about disclosures of government data requests. Apple was represented by General Counsel Bruce Sewell and two other employees, according to people who were there. The following account of what happened at the meeting is based on recollections of those people.

In his fourth-floor conference room, Mr. Cole told the Apple officials they were marketing to criminals.

At one point, he read aloud from a printout of Apple's announcement, quoting a section in which the company said that under the new system Apple couldn't cooperate with a court order to retrieve data from a phone even if it wanted to.

Mr. Cole offered the Apple team a gruesome prediction: At some future date, a child will die, and police will say they would have been able to rescue the child, or capture the killer, if only they could have looked inside a certain phone.

His statements reflected concern within the FBI that a careful criminal can shield much activity from police surveillance by minimizing use of cellphone towers and not backing up data.

The Apple representatives viewed Mr. Cole's suggestion as inflammatory and inaccurate. Police have other ways to get information, they said, including call logs and location information from cellphone carriers. In addition, many users store copies of a phone's data elsewhere.

During the hourlong meeting, Mr. Sewell said Apple wasn't marketing to criminals, but to ordinary consumers who store growing amounts of data about themselves on smartphones and are increasingly suspicious of tech companies. Many of those customers are outside the U.S., the Apple representatives said, where phone users want to shield information from governments that are less respectful of individual rights.

If the government wants more information from Apple, the company representatives said, it should change the law to require all companies that handle communications to provide a means for law enforcement to access the communications.

Mr. Cole predicted that would happen, after the death of a child or similar event.

More than once, Mr. Cole suggested there had to be a technical solution—a way to design a phone so that police, with a court order, can access information, without compromising security.

"We can't create a key that only the good guys can use," Mr. Sewell responded.

After the meeting, Mr. Cole told colleagues he didn't expect Apple to back down.

The two sides agreed to a follow-up meeting between technical experts from Apple and the Justice Department. At that meeting, Apple laid out ways in which the government could still collect information about specific phones. But its representatives acknowledged that under the new system, there will be more information on the phones that can be hidden from investigators, even with a warrant.

Later in October, Mr. Comey, the FBI director, criticized the new Apple and Google encryption schemes in a speech, saying the pendulum had swung too far toward protecting privacy, at the expense of law enforcement.

At Apple, Mr. Cook believes consumers will push the pendulum further toward protecting privacy. At the Journal conference, he made a prediction: Consumers will appreciate efforts to protect their privacy once "something major happens."

"When that happens everybody wakes up and says, 'Oh my God,' and they make a change," he said. "What that event is, I don't know, but I'm pretty convinced that it's going to happen."

During discussions inside the White House, some officials disagreed with Mr. Comey's approach, according to people familiar with those talks. They had urged the FBI not to speak out publicly, arguing the best chance at a policy change was through quiet negotiations, these people said. Obama administration officials say they plan to keep talking with the tech companies about the issues.

In the debate over phones, government officials repeatedly cite kidnapping or child-abuse cases, in an effort to make law enforcement the focus of the debate, rather than national security. Terror suspects with better-protected data are a serious concern, officials say, but they believe catching criminals is a better public argument to make.

In his October speech, the FBI's Mr. Comey cited the case of a murdered boy, whom he didn't name, as one example where data taken from a phone was critical to solving a crime.

That boy, it later emerged, was 12-year-old Justin Bloxom, who was murdered in 2010 in Mansfield, La. His mother, Amy Fletcher, says she has no doubt that phone evidence was critical in convicting his killer. "Everything that was done was done through texts from a damn cellphone," she says.

Investigators quickly focused on Brian Horn, a cabdriver and convicted sex offender. Mr. Horn's cellphone was recovered by investigators and sent to the FBI for analysis. The texts showed Mr. Horn lured the boy into his cab by pretending to be a 15-year-old girl looking for sex.

Mr. Horn's lawyer, Daryl Gold, calls the phone "a crucial piece of evidence." Before investigators recovered it, he said, "They had a totally circumstantial case." Mr. Horn was convicted and sentenced to death. He is appealing.

Weighing in on the Encryption and "Going Dark" Debate

Lawfare Blog, By Carrie Cordero, Thursday, December 4, 2014 at 11:30 AM

Yesterday I took part in a panel discussion entitled "Device Encryption: Too Much Privacy for Consumers?" hosted by the Future of Privacy Forum (FPF) and the International Association of Privacy Professionals (IAPP). The discussion focused on the reinvigorated "going dark" debate, in light of recent steps by Apple and Google (and presumably, others to come) to build-in encryption to a variety of services, thereby making the companies incapable of responding to lawful court orders in criminal and national security matters. Hogan Lovells Partner and FPF Founder Christopher Wolf moderated the conversation which included Cato's Julian Sanchez and Access' Amie Stepanovich. This post summarizes some of my observations related to that discussion.

While the going dark issue is not new, there are important differences between today's discussion versus those of the 1990s or even 2011, when former FBI General Counsel (now federal district court judge) Valerie Caproni testified before Congress on the issue. While we know that there are significant differences between the going dark debate of the 1990s and now, given the changes in communications technology, what may not be as obvious are the differences in the policy discussion between as recent as 2011, and today. More specifically, three policy positions put forth by the FBI in 2011 likely have shifted, or are about to shift:

First, in 2011, the FBI was primarily concerned about technological challenges impeding real-time interception, i.e. electronic surveillance. Today, access to stored data, including data stored in mobile phones/devices, is clearly on the table.

Second, in 2011, the FBI General Counsel stated that changes to encryption technology were not required. Today, given the aggressive and accelerated deployment of encryption by the leading communications service providers, encryption practice and policy is necessarily up for discussion.

Third, in 2011, the FBI viewed its legislative authorities as sufficient. Although there is no current Administration proposal to amend the 1994 CALEA, FBI Director Comey's stated in his remarks at Brookings in October that "we also need a regulatory or legislative fix to create a level playing field…." Accordingly, if the Executive Branch cannot come to informal working agreements with the technology industry (which seems unlikely in the current environment), we may be looking at a legislative debate sooner rather than later.

The crux of the current debate is this: if industry refuses to cooperate voluntarily, is there a societal interest in mandating by law that companies preserve the technical capability to respond to lawful court orders to prevent, investigate and prosecute crimes, and to protect against terrorism and other national security threats? The technology industry appears to be moving in the direction of building-in encryption technology for everyday consumers that may make it impossible for law enforcement authorities to access devices. As yesterday's panel discussion revealed, concerns about national security surveillance revealed by the Snowden disclosures are driving the industry reaction. But the chief law enforcement officer wants to be able to access the devices with a court order or warrant, leaving allegations of "mass surveillance" flat.

This summer, the Supreme Court held in Riley that a warrant is required for a search of a cell phone, even when the search is incident to arrest. But the Court also recognized a legitimate government need for lawful execution of search warrants. The Court said:

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency." (Riley at 26-27, citing Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971).)

So how will the debate proceed? Hopefully, with more facts demonstrating that the issues raised by the FBI Director present real impediments to preventing, investigating and prosecuting serious crimes and protecting the country against national security threats. It will take more than a sampling of case anecdotes to make the case. During the 1994 legislative debate over CALEA, FBI Director Freeh presented a variety of statistics and categories that were not just based on FBI anecdotal experience, but included statistics regarding the thwarting of investigations across federal law enforcement as well as state and local law enforcement. In addition, CALEA's legislative history reveals that GAO conducted an independent review and concluded that the technological situation at the time presented real impediments to lawful investigations.

Apple's dangerous game

The Washington Post, By Orin Kerr, September 19, 2014

[Note to readers: I changed my views after receiving feedback to this post…***CDA Editor***: Find Kerr's subsequent posts by looking up this article (Google "Kerr Apple's Dangerous Game"). They reconsider but do not invalidate these arguments.]

Apple has announced that it has designed its new operating system, iOS8, to thwart lawful search warrants. Under Apple's old operating system, if an iPhone is protected by a passcode that the government can't bypass, the government has to send the phone to Apple together with a search warrant. Apple will unlock at least some of the contents of the phone pursuant to the warrant. Under the new operating system, however, Apple has devised a way to defeat lawful search warrants. "Unlike our competitors," Apple's new privacy policy boasts, "Apple cannot bypass your passcode and therefore cannot access this data." Warrants will go nowhere, as "it's not technically feasible for [Apple] to respond to government warrants for the extraction of this data from devices in their possession running iOS 8." Anyone with any iPhone can download the new warrant-thwarting operating system for free, and it comes automatically with the new iPhone 6.

I find Apple's new design very troubling. In this post, I'll explain why I'm troubled by Apple's new approach coded into iOS8. I'll then turn to some important legal issues raised by Apple's announcement, and conclude by thinking ahead to what Congress might do in response.

Let's begin with a really important point: In general, cryptography is an awesome thing. Cryptography protects our data from hackers, trespassers, and all sorts of wrongdoers. That's hugely important. And under Apple's old operating system, cryptography protects iPhones from rogue police officers, too. Thanks to the Supreme Court's recent decision in Riley v. California, the Fourth Amendment requires a warrant to search a cell phone. Apple's old operating system effectively enforced the warrant requirement technologically by requiring the government to serve a warrant on Apple to decrypt the phone.

Up to that point, I think it's all good. But the design of Apple's new operating system does something really different.

If I understand how it works, the only time the new design matters is when the government has a search warrant, signed by a judge, based on a finding of probable cause. Under the old operating system, Apple could execute a lawful warrant and give law enforcement the data on the phone. Under the new operating system, that warrant is a nullity. It's just a nice piece of paper with a judge's signature. Because Apple demands a warrant to decrypt a phone when it is capable of doing so, the only time Apple's inability to do that makes a difference is when the government has a valid warrant. The policy switch doesn't stop hackers, trespassers, or rogue agents. It only stops lawful investigations with lawful warrants.

Apple's design change one it is legally authorized to make, to be clear. Apple can't intentionally obstruct justice in a specific case, but it is generally up to Apple to design its operating system as it pleases. So it's lawful on Apple's part. But here's the question to consider: How is the public interest served by a policy that only thwarts lawful search warrants?

The civil libertarian tradition of American privacy law, enshrined in the Fourth Amendment, has been to see the warrant protection as the Gold Standard of privacy protections. The government can't invade our private spaces without a showing that the invasion is justified by the expectation that the search will recover evidence. And the government must go to a neutral magistrate and make that case before it conducts the search. When the government can't make the showing to a neutral judge, the thinking runs, the public interest in privacy outweighs the public interest in solving crime. But when the government does make that showing, on the other hand, the public interest in solving crime outweighs the privacy interest. That's the basic balance of the Fourth Amendment, most recently found in the stirring civil libertarian language in Riley just a few months ago.

Apple's new policy seems to thumb its nose at that great tradition. It stops the government from being able to access the phone precisely when it has a lawful warrant signed by a judge. What's the public interest in that?

One counterargument I have heard is that there are other ways the government can access the data at least some of the time. With the warrant required under Riley, agents could take a stab at guessing the passcode. Perhaps the phone's owner used one of the popular passwords; according to one study, the top 10 most often-used passcodes will unlock about 15% of phones. Alternatively, if the phone's owner has backed up his files using iCloud, Apple will turn over whatever has been backed up pursuant to a lawful warrant.

These possibilities may somewhat limit the impact of Apple's new policy. But I don't see how they answer the key question of what's the public interest in thwarting valid warrants. After all, these options also exist under the old operating system when Apple can comply with a warrant to unlock the phone. And while the alternatives may work in some cases, they won't work in other cases. And that brings us back to how it's in the public interest to thwart search warrants in those cases when the alternatives won't work. I'd be very interested in the answer to that question from defenders of Apple's policy. And I'd especially like to hear an answer from Apple's General Counsel, Bruce Sewell.

Let me conclude with two important legal questions raised by Apple's new policy, together with some speculation about how Congress might respond to Apple's change.

The first question is whether the government can lawfully compel the telephone's owner to divulge the passcode. I believe the answer is that yes, a person can in fact face punishment for refusal to enter in the password to decrypt his own phone. If the government obtains a subpoena ordering the person to enter in the passcode, and the person refuses or falsely claims not to know the passcode, a person can be held in contempt for failure to comply.

Some may think that the Fifth Amendment right against self-incrimination prohibits such punishment. But I think that's wrong because of the specific circumstances in which the issue arises. Because people must know their passcodes to use their own phones, the testimonial aspect of decrypting a person's own phone — admitting that the phone belongs to them and they know the password — will be a "foregone conclusion" whenever the government can show that the phone belongs to that person. If the phone's in the suspect's hand or in his pocket when the government finds it, that's not going to be hard to show. Under the relevant case law, that makes all the difference: Entering in the password no longer raises a Fifth Amendment problem. See, e.g, In re Boucher, 2009 WL 424718 (D.Vt. 2009).

A second question is how the new policy changes the rules for searching a cell phone incident to arrest. Under the Supreme Court's recent decision in Riley, the government needs a warrant to search the phone. But under the new Apple policy, warrants to search the phone won't work if the passcode is in place. If officers lawfully come into possession of a target's unlocked phone, the data may effectively disappear as soon as the phone locks. It's kind of the digital equivalent of flushing the drugs down the toilet, but it happens by default and automatically. This will create interesting questions under the exigent circumstances exception. If officers make an arrest and the phone hasn't yet locked, does the exigent circumstances exception now allow the police to search the phone without a warrant because the delay of waiting for a warrant will mean a locked phone that can't be unlocked even with a warrant? At least in some circumstances, such as when the government has probable cause and the screensaver suggests a later iOS operating system, I suspect the answer may be yes. (Incidentally, I have long argued that the Supreme Court should wait until a technology stabilizes before applying the Fourth Amendment to it to avoid the problem of announcing a rule that doesn't make sense over time. In light of Apple's new iOS8, Riley may be an interesting example.)

I'll conclude with the interesting question of Congressional reaction. It may turn out that the government can get access to the data most of the time despite this new policy using a combination of unlocked phones, data from backups in the cloud, password-guessing, or compelling targets to unlock their phones. If the government can get to the data in other ways, then the Apple policy may not cause much outrage. The government will muddle through. Perhaps.

But imagine that the Apple policy thwarts a lot of important cases. Think of a homicide case in which the government wants to search the victim's phone for evidence of who was behind the killing. Maybe the victim received a text message that provides the key to the case, and the cellular provider hasn't stored the messages. Because the victim isn't alive to share his password, and the phone will have locked before the body was found, the government won't be able to search the phone to find the messages. Apple's policy will keep the police from finding the killer. That seems bad.

If we get a lot of cases like that, I suspect Congress may look to legislation to try to restore the privacy/security balance more in the direction of the traditional Fourth Amendment warrant requirement. I can think of three paths Congress might take. To be clear, I'm not endorsing any approach, at least yet. I'm just covering the major options. They look like this:

1) The most obvious option would be follow the example of CALEA and E911 regulations by requiring cellular phone manufacturers to have a technical means to bypass passcodes on cellular phones. In effect, Congress could reverse Apple's policy change by mandating that phones be designed to have this functionality. That would restore the traditional warrant requirement.

2) A second option would be to enact a new law severely punishing a target's refusal to enter in his passcode to decrypt his phone. Under current law, such a refusal could lead to civil or criminal contempt charges. But given that the Fifth Amendment isn't implicated for reasons discussed above, I don't think there is a constitutional barrier to punishing it more severely. How severely is a policy question up to Congress, so Congress could theoretically impose quite high punishments. Of course, this option wouldn't work if the owner of the phone is unavailable, such as would be the case in a homicide investigation when it's the victim's phone.

3) A third option would be to impose data retention laws. If the key evidence lost because of Apple's policy is communications data stored on the phone that won't be found elsewhere, Congress could require providers to store the data. For example, Congress could require cell providers to retain specific kinds of data (such as text messages) so it can obtain the messages from the provider with a warrant rather than from the phone.

Anyway, that's my take, which I'm happy to open up for comments and reactions. Perhaps I'm misunderstanding Apple's policy. If so, I'll post a correction and apologize for wasting everyone's time with such a long post. But at least based on my understanding of the policy, it strikes me as troubling. And if the switch ends up thwarting a lot of valid investigations, I suspect Apple may not have the last word.

Orin Kerr is the Fred C. Stevenson Research Professor at The George Washington University Law School, where he has taught since 2001. He teaches and writes in the area of criminal procedure and computer crime law.

Is Apple Picking a Fight With the U.S. Government? Not Exactly

Slate: Future Tense, Sep. 23, 2014, By Matthew Green

Last week Apple released its new iOS 8 operating system for iPhones, iPads, and iPod Touch devices. Most of the coverage of iOS 8 focuses on visible features that users can interact with. But there's one major change in iOS 8 that most users probably won't notice unless they find themselves in a great deal of trouble. Specifically, Apple has radically improved the way that data on those devices is encrypted. Once users set a passcode, Apple will no longer be able to unlock your device—even if ordered to do so by a court.

While privacy advocates have praised Apple's move, it has drawn fire from some notable legal scholars. Writing in the Washington Post on Sept. 19, Orin Kerr referred to Apple's new policy as a "dangerous game," one that "doesn't stop hackers, trespassers, or rogue agents" but "only stops lawful investigations with lawful warrants." While Kerr has moderated his views since his initial post, his overarching concern remains the same: By placing customer interests before that of law enforcement, Apple is working against the public interest. If you interpret Apple's motivations as Kerr does, then Apple's recent move is pretty surprising. Not only has the company picked a pointless fight with the United States government, it's potentially putting the public at risk.

The only problem is that Kerr is wrong about this. Apple is not designing systems to prevent law enforcement from executing legitimate warrants. It's building systems that prevent everyone who might want your data—including hackers, malicious insiders, and even hostile foreign governments—from accessing your phone. This is absolutely in the public interest. Moreover, in the process of doing so, Apple is setting a precedent that users, and not companies, should hold the keys to their own devices.

To see why this is the case, you need to know a bit about what Apple is doing with its new technology. The first time you power up a new iPhone or iPad, you'll be asked to set a passcode for unlocking your phone. This can be a full password or

just a 4-digit PIN (though the former is certainly stronger). On devices with a Touch ID sensor, you'll also be allowed to use your fingerprint as a more convenient alternative.

A passcode may look like flimsy security, but it's not. The minute you set one, Apple's operating system immediately begins encrypting your phone's sensitive data—including mail, texts, photos, and call records—using a form of encryption that the U.S. government uses to protect classified military secrets. The key for this encryption is mathematically derived by combining your passcode with a unique set of secret numbers that are baked into your phone.

If all goes well, you'll never notice this is happening. But the impact on data raiders is enormous. Even if someone cracks your phone open and attempts to read data directly off of the memory chips, all she'll see is useless, scrambled junk. Guessing your passcode won't help her—unless she can also recover the secret numbers that are stored within your phone's processor. And Apple's latest generation of phones makes that very difficult. Of course, your would-be data thief could try to get in by exhaustively trying all possible combinations, but according to an iOS security document, Apple also includes protections to slow this attack down. (In the same document, Apple estimates that a 6-digit alphanumeric password could take upward of five years to guess.)

That's the problem with keys. If you have them, sooner or later someone is going to ask you to use them.

The encryption on Apple devices is not entirely new with iOS 8. What is new is the amount of data your phone will now encrypt. Apple has extended encryption protections to nearly all the data you produce on a daily basis and will also require you to enter the passcode (or fingerprint) each time you reboot your phone. In addition, if you purchase a recent iPhone (5S, 6, or 6 Plus), Apple will store your keys within a dedicated hardware encryption "co-processor" called the Secure Enclave.

Taking Apple's recent privacy announcements at face value, even Apple itself can't break into the Secure Enclave in your phone. While it may seem "natural" that the designer of a system—in this case Apple—can break its own encryption, the truth is that such a capability is hardly an inevitable design outcome. For Apple to maintain such a capability with its newer security processors, it can't just be more knowledgeable than its customers. It would have to literally design in a form of "skeleton key." In computer security circles this mechanism is generally known as a "backdoor."

Designing backdoors is easy. The challenge is in designing backdoors that only the right people can get through. In order to maintain its access to your phone, Apple would need a backdoor that allowed them to execute legitimate law enforcement requests, while locking hackers and well-resourced foreign intelligence services out. The problem is so challenging that even the National Security Agency has famously gotten it wrong.

To dive into the technical weeds, any backdoor Apple might design would likely require the company to store some sort of master access key—or even a whole database of such keys, one for every phone it sells. In the worst case, these keys might need to be carefully transported from the factory in China, to a locked and guarded room at Apple HQ in Cupertino, California. They would be kept isolated from the Internet to protect them from hackers, and Apple would have to constantly monitor its own employees to prevent abuse. None of this is cheap, and the stakes are high: A data breach involving Apple's master keys could catastrophically harm the company's reputation, particularly in the security-conscious enterprise market.

Much of the Apple criticism thus far stems from the perception that Apple is primarily targeting the U.S. government with its new encryption features. But this is shortsighted. Apple currently has retail stores in 14 countries and sells its phones in many more. The United States is not the only government with law enforcement, or with an interest in its citizens' data.

Fortunately we don't have to speculate about what those interests might be. Back in 2012, rumors swirled that the Indian government had threatened to ban BlackBerry's messaging services and had even forced BlackBerry to hand over the encryption keys to that service. BlackBerry denied handing over the keys, but eventually admitted it had built a "lawful intercept" mechanism for the Indian government.

If Apple holds its customers' keys (or maintains a backdoor into your phone), then the same calculus will soon apply to Apple. That's the problem with keys. Once you have them, sooner or later someone will expect you to use them. Today those requests originate from police in the United States. Tomorrow they may come from the governments of China or Russia. And while those countries certainly have legitimate crime to prosecute, they're also well known for using technology to persecute dissidents. Apple may not see either public interest or shareholder value in becoming the world's superintendent—meekly unlocking the door for whichever nation's police ask them to.

Apple's new encryption may not solve this problem entirely—foreign governments could always ban the sale of Apple products or force Apple to redesign. But by approaching the world with a precedent that customers, not Apple, are responsible for the security of their phones, Apple can at least make a credible attempt to stay above the fray.

Disclosure: I have served as an expert witness in court cases that involve Apple technology, though I have neither worked for Apple nor do I have access to any nonpublic information about Apple's encryption technology.

Matthew Green is a research professor of computer science at Johns Hopkins University. His research focuses on applied cryptography and computer security.

FBI blasts Apple, Google for locking police out of phones

The Washington Post, By Craig Timberg and Greg Miller September 25, 2014

FBI Director James B. Comey sharply criticized Apple and Google on Thursday for developing forms of smartphone encryption so secure that law enforcement officials cannot easily gain access to information stored on the devices — even when they have valid search warrants.

His comments were the most forceful yet from a top government official but echo a chorus of denunciation from law enforcement officials nationwide. Police have said that the ability to search photos, messages and Web histories on smartphones is essential to solving a range of serious crimes, including murder, child pornography and attempted terrorist attacks.

"There will come a day when it will matter a great deal to the lives of people . . . that we will be able to gain access" to such devices, Comey told reporters in a briefing. "I want to have that conversation [with companies responsible] before that day comes."

Comey added that FBI officials already have made initial contact with the two companies, which announced their new smartphone encryption initiatives last week. He said he could not understand why companies would "market something expressly to allow people to place themselves beyond the law."

Comey's remarks followed news last week that Apple's latest mobile operating system, iOS 8, is so thoroughly encrypted that the company is unable to unlock iPhones or iPads for police. Google, meanwhile, is moving to an automatic form of encryption for its newest version of Android operating system that the company also will not be able to unlock, though it will take longer for that new feature to reach most consumers.

Both companies declined to comment on Comey's remarks. Apple has said that its new encryption is not intended to specifically hinder law enforcement but to improve device security against any potential intruder.

For detectives working a tough case, few types of evidence are more revealing than a smartphone. Call logs, instant messages and location records can link a suspect to a crime precisely when and where it occurred. And a surprising number of criminals, police say, like to take selfies posing with accomplices — and often the loot they stole together.

But the era of easy law enforcement access to smartphones may be drawing to a close as courts and tech companies erect new barriers to police searches of popular electronic devices. The result, say law enforcement officials, legal experts and forensic analysts, is that more and more seized smartphones will end up as little more than shiny paperweights, with potentially incriminating secrets locked inside forever.

The irony, some say, is that while the legal and technical changes are fueled by anger over reports of mass surveillance by the National Security Agency, the consequences are being felt most heavily by police detectives, often armed with warrants certifying that a judge has found probable cause that a search of a smartphone will reveal evidence of a crime.

"The outrage is directed at warrantless mass surveillance, and this is a very different context. It's searching a device with a warrant," said Orin Kerr, a former Justice Department computer crimes lawyer who is now a professor at George Washington University.

Not all of the high-tech tools favored by police are in peril. They can still seek records of calls or texts from cellular carriers, eavesdrop on conversations and, based on the cell towers used, determine the general locations of suspects. Police can seek data backed up on remote cloud services, which increasingly keep copies of the data collected by smartphones. And the most sophisticated law enforcement agencies can deliver malicious software to phones capable of making them spy on users.

Yet the devices themselves are gradually moving beyond the reach of police in a range of circumstances, prompting ire from investigators. Frustration is running particularly high at Apple, which made the first announcement about new encryption and is moving much more swiftly than Google to get it into the hands of consumers.

"Apple will become the phone of choice for the pedophile," said John J. Escalante, chief of detectives for Chicago's police department. "The average pedophile at this point is probably thinking, I've got to get an Apple phone."

The rising use of encryption is already taking a toll on the ability of law enforcement officials to collect evidence from smartphones. Apple in particular has been introducing tough new security measures for more than two years that have made it difficult for police armed with cracking software to break in. The new encryption is significantly tougher, experts say.

"There are some things you can do. There are some things the NSA can do. For the average mortal, I'd say they're probably out of luck," said Jonathan Zdziarski, a forensics researcher based in New Hampshire.

Los Angeles police Detective Brian Collins, who does forensics analysis for anti-gang and narcotics investigations, says he works on about 30 smartphones a month. And while he still can successfully crack into most of them, the percentage has been gradually shrinking — a trend he fears will only accelerate.

"I've been an investigator for almost 27 years," Collins said, "It's concerning that we're beginning to go backwards with this technology."

The new encryption initiatives by Apple and Google come after June's Supreme Court ruling requiring police, in most circumstances, to get a search warrant before gathering data from a cellphone. The magistrate courts that typically issue search warrants, meanwhile, are more carefully scrutinizing requests amid the heightened privacy concerns that followed the NSA disclosures that began last year.

Civil liberties activists call this shift a necessary correction to the deterioration of personal privacy in the digital era — and especially since Apple's introduction of the iPhone in 2007 inaugurated an era in which smartphones became remarkably intimate companions of people everywhere.

"Law enforcement has an enormous range of technical and old-fashioned methods to go after the perpetrators of real crime, and no amount of security effort at Silicon Valley tech companies is going to change that fact," said Peter Eckersley, director of technology projects at the Electronic Frontier Foundation, a civil liberties group based in San Francisco. "The reality is that if the FBI really wants to investigate someone, they have a spectacular arsenal of weapons."

Sometimes, police say, that's not enough.

Escalante, the Chicago chief of detectives, pointed to a case in which several men forced their way into the home of a retired officer in March and shot him in the face as his wife lay helplessly nearby. When the victim, Elmer Brown, 73, died two weeks later, city detectives working the case already were running low on useful leads.

But police got a break during a routine traffic stop in June, confiscating a Colt revolver that once belonged to Brown, police say. That led investigators to a Facebook post, made two days after the homicide, in which another man posed in a cellphone selfie with the same gun.

When police found the smartphone used for that picture, the case broke open, investigators say. Though the Android device was locked with a swipe code, a police forensics lab was able to defeat it to collect evidence; the underlying data was not encrypted. Three males, one of whom was a juvenile, eventually were arrested.

"You present them with a picture of themselves, taken with the gun, and it's hard to deny it," said Sgt. Richard Wiser, head of the Chicago violent crimes unit that investigated the case. "It played a huge role in this whole thing. As it was, it took six months to get them. Who knows how long it would have taken without this."

Craig Timberg is a national technology reporter for The Post.

Russian police offer $37,000 bounty to hack iPhone encryption

By Chuong H Nguyen, Tuesday, Dec 2, 2014, iMore.com

Not only are U.S. law enforcement officials fighting Apple on iPhone encryption for criminal cases, it appears that the Russian police want to be able to hack Apple's smartphones in a similar effort to fight crime. Russian authorities are reportedly buying equipment that will enable them to hack Apple's iOS encryption, and officials are also offering a $37,000 bounty to whomever could hack the phones.

As reported on RT News: "If Apple products were to be used to commit crime, this equipment would help experts to search such a device for information pertaining to a criminal investigation," police spokesperson Nina Pelevina told Komsomolskaya Pravda newspaper.

Source: RT News (RT is a Russian state-funded television network which runs cable and satellite television channels, as well as Internet content directed to audiences outside the Russian Federation. Wikipedia)

Tech firms freak out as China erects barriers

By Virginia Harrison, CNNMoney (London) February 26, 2015: 2:22 PM ET

Western companies are starting to freak out about moves by China that could prevent them supplying the country's financial industry with technology. Six groups representing European companies and banks have appealed for official help this week. They say China is breaking international trade rules. That comes as Beijing is reported to be removing some of the world's top tech brands from a list of approved central government suppliers.

China unveiled plans to regulate banking technology late last year. The rules, which are due to come into force next month, could require tech companies to share source code and other proprietary information with Beijing. The European business lobby groups want the European Commission to help get the regulations suspended. They say the policies would "hurt the

development and integration of Chinese banking sector in the global market."

"Combined with China's recent other actions to tighten content filters and limit Internet-based services, these new policies will create an even more unwelcoming digital trade and investment environment for foreign companies," the groups wrote in a letter to the European Commission.

A spokesperson said the European Commission is analyzing the Chinese measures and their potential impact. "We are in regular contact with the Chinese authorities on trade matters and will certainly raise this issue," the spokesperson said.

One of the authors of the letter -- Business Europe director general Markus Beyrer -- told CNNMoney his group was "particularly concerned about the potential for these measures to be applied to other sectors."

Reuters reported Wednesday that China had removed Cisco (CSCO, Tech30), Apple (AAPL, Tech30), Citrix Systems (CTXS) and Intel's (INTC, Tech30) security software provider McAfee from an approved procurement list. These companies will now have to fight for contracts worth less than $80,000 that previously may have been awarded without a competitive process.

"Cisco is allowed to sell to all Chinese government, enterprise, and commercial customers. Any suggestion otherwise is false," said a Cisco spokesman. "We have served our customers in China for more than 20 years, and we look forward to continuing to do so."

The number of approved foreign brands dropped by one third last year, according to the Reuters report.

Relations with the U.S. have been strained by revelations from Edward Snowden that the government relies on American tech firms to spy on Chinese leaders.

The U.S. has repeatedly blocked Chinese telecom company Huawei from proposed acquisitions and partnerships -- including a bid for 3Com and a supply deal with Sprint (S) -- because it accuses it of spying.

Communications Assistance for Law Enforcement Act

From Wikipedia, the free encyclopedia

The Communications Assistance for Law Enforcement Act (CALEA) is a United States wiretapping law passed in 1994, during the presidency of Bill Clinton (Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010).

CALEA's purpose is to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to wiretap any telephone traffic; it has since been extended to cover broadband internet and VoIP traffic. Some government agencies argue that it covers monitoring communications rather than just tapping specific lines and that not all CALEA-based access requires a warrant; this is of course highly controversial.

The original reason for adopting CALEA was the Federal Bureau of Investigation's worry that increasing use of digital telephone exchange switches would make tapping phones at the phone company's central office harder and slower to execute, or in some cases impossible.[citation needed] Since the original requirement to add CALEA-compliant interfaces required phone companies to modify or replace hardware and software in their systems, U.S. Congress included funding for a limited time period to cover such network upgrades.[citation needed] CALEA was passed into law on October 25, 1994 and came into force on January 1, 1995.[citation needed]

In the years since CALEA was passed it has been greatly expanded to include all VoIP and broadband internet traffic. From 2004 to 2007 there was a 62 percent growth in the number of wiretaps performed under CALEA — and more than 3,000 percent growth in interception of internet data such as email.[1]

By 2007, the FBI had spent $39 million on its DCSNet system, which collects, stores, indexes, and analyzes communications data.[1]