Testimony for
House Judiciary Committee Hearing on
"The Encryption Tightrope: Balancing Americans' Security and Privacy"
March 1, 2016

Susan Landau, PhD
Professor of Cybersecurity Policy
Worcester Polytechnic Institute
100 Institute Road
Worcester MA 01609

Testimony for

House Judiciary Committee Hearing on

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

March 1, 2016

Mr. Chairman and Members of the Committee:

Thank you very much for the opportunity to testify today on "The Encryption Tightrope: Balancing Americans' Security and Privacy." My name is Susan Landau, and I am professor of cybersecurity policy at Worcester Polytechnic Institute. I have previously been a Senior Staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems. I am the author of two books on the issues of today's hearing: *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998); the latter is co-authored with Whitfield Diffie. I have written about these issues in the *Washington Post, the Chicago Tribune, Scientific American*, and other venues. I am a Fellow of the Association for Computing Machinery and of the American Association for the Advancement of Science, and I was recently inducted into the Cybersecurity Hall of Fame.[1]

My comments represent my own views and not those of the institutions with which I am affiliated.

Today I will speak on security threats, encryption, and securing smartphones.

It would seem to be a fairly straightforward issue: the smartphone of one of the two San Bernardino terrorists had its data encrypted. Because Apple designed the phone to be secure—and to destroy its data if there were ten incorrect tries of the PIN to unlock it—the FBI cannot unlock the smartphone (or at least cannot without risking destroying the data). The court has ordered Apple to create a phone update that

[1] Additional biographical information relevant to the subject matter to the hearing: I am also a Visiting Professor of Computer Science at University College London. For over two decades I have been studying encryption policy and the risks that occur when wiretapping capabilities are embedded in communications infrastructures. At Sun I was involved in issues related to cryptography and export control, security and privacy of federated identity management systems, and in developing our policy stance in digital rights management. I serve on the National Research Council Computer Science and Telecommunications Board, and recently participated in an Academies study on *Bulk Signals Intelligence Collection: Technical Alternatives* (2015). I have served on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering (2009-2012), the Commission on Cyber Security for the 44th Presidency (2009-2011), and the National Institute of Standards and Technology's Information Security and Privacy Advisory Board (2002-2008). I hold a PhD in applied math/theoretical computer science from MIT.

will undo this and other security aspects of the software, thus enabling the FBI to brute force the key to reveal whatever information is on the phone.

But little in cyber is straightforward. Despite appearances, this is not a simple story of national security versus privacy. It is, in fact, a security versus security story although there are, of course, aspects of privacy embedded in it as well.

The way we use our phones is very different than a decade ago; they are, as the Supreme Court observed in *Riley v. California,*[2] "minicomputers that also happen to have the capacity to be used as a telephone. [The phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers'." Smartphones are already holders of account information (financial and otherwise), and are poised to become authenticators to a wide variety of services we access via the Internet.

And that is why we have a security versus security story. The Internet has brought huge benefits, but it has also vastly simplified attacks and exploits.[3] Cyberespionage netted Chinese military a "huge amount of design and electronics data on the F-35,"[4] Russian intrusions[5] into law firms[6] (the target here likely to be patent filings), an Iranian hacker probing US critical infrastructure (with possible intent to attack)[7] are examples. Each day brings more news of such attacks and exploits.

The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. In the last decade, the United States has been under an unprecedented attack, one that NSA Director Keith Alexander has called "the greatest transfer of wealth in history."[8]

---

[2] 134 S. Ct. 2473 (2014).

[3] It might be hard to understand why a network on which society has become so dependent is so insecure. The short answer is history. The ARPANet, the precursor to the Internet, began as a research network on which everyone was a trusted partner. When the NSFnet, the follow-on network to the ARPANet, was opened up to commercial traffic, it relied on the same protocols. These assumed a trusted user body, which was not really sensible for a network that would support financial transactions, manage critical infrastructure, and the like.

[4] David Alexander, "Theft of F-35 design data is helping US adversaries—Pentagon," *Reuters*, June 19, 2013.

[5] Director of National Intelligence James Clapper views Russia as the top cyber threat. See, e.g., Siobhan Gorman, "Intel Chief: Russia Tops China as Cyber Threat," *Wall Street Journal*, October 17, 2014.

[6] Mandiant Consulting, "M-Trends 2016: Special Report," p. 45, https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

[7] Stephanie Gosk, Tom Winter, and Tracy Connor, "Iranian Hackers Claim Cyber Attack on US Dam," NBC News, December 23, 2015.

[8] Josh Rogin, "NSA Chief: Cybercrime constitutes 'greatest transfer of wealth in history'," *The Cable,* July 9, 2012.

Stealing your login credentials provides criminals and nation states the most effective way into your system—and a smartphone provides one of the best ways of securing ourselves.

That's why Apple's approach to securing phone data is so crucial.

But law enforcement continues to see electronic surveillance in twentieth century terms, and it is using twentieth-century investigative thinking in a twenty-first century world. Instead of celebrating steps industry takes to provide security to data and communications, the FBI fights it.

I should note that this response is different from NSA's, which over the last two decades, has, despite public perception, both encouraged and aided industry's efforts in securing communications.[9]

Instead of embracing the communications and device security we so badly need for securing US public and private data, law enforcement continues to press hard to undermine security in the misguided desire to preserve simple, but outdated, investigative techniques.

There is another way. Law enforcement should embrace the protections that industry is implementing to secure private—and, because of wide adoption, also government—sector data and develop substantive advanced capabilities to conduct investigations when needed. In the late 1990s, the NSA faced similar challenges and overcame them.[10]

We need twenty-first century technologies to secure the data that twenty-first century enemies—organized crime and nation-state attackers—seek to steal and exploit. Twentieth century approaches that provide law enforcement with the ability to investigate but also simplify exploitations and attacks are not in our national-security interest.[11] Instead of laws and regulations that weaken our protections, we should enable law enforcement to develop twenty-first century capabilities for conducting investigations.

Now I should note that the FBI already has some excellent capabilities in this area. But FBI investment and capacity in this area is not at the scale and level necessary to be as effective as it needs to be.

---

[9] This is true despite the fact that the NSA has also sought to undermine some protections; see later in this testimony as well as Susan Landau "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

[10] See, e.g., Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

[11] For a humorous take on these issues, see The Strip, New York Times, February 28, 2016, http://www.nytimes.com/slideshow/2012/07/08/opinion/sunday/the-strip.html#1

That's where Congress can help. Law enforcement must develop the capability for conducting such investigations themselves (or through a combination of in house and carefully managed contracting). Though there have been nascent steps in this direction by law enforcement, a much larger and complete effort is needed. Help the FBI build such capabilities, determine the most efficient and effective way that such capabilities can be utilized by state and local law enforcement, and fund it.

This is the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can to develop better, more effective technologies for securing data and devices. This is a win/win, and where we should be going.

The rest of my testimony presents details of these concerns. Thank you very much for the opportunity to address you on this critical national-security topic.

Understanding our Security Threat

When terrorists wearing tactical gear and black masks and armed with guns and bombs attack a concert hall or Christmas party, our immediate emotional reaction is that we must move heaven and earth to prevent future such attacks. The role of leadership includes making choices. Here we are faced with a situation where logic and analysis lead to a different calculus on safety and security than do emotions. So while FBI Director James Comey has argued that, "We could not look the survivors in the eye if we did not follow this lead,"[12] this view is a mistaken view of where our most serious risks as a nation lie. Page one of the 2016 Department of Defense Threat Assessment states: "Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems."[13]

This is why securing communications and devices is so very crucial, and it is where the situation grows complicated. Despite our deeply human tendency to react to the attack that is occurring right now, we must focus and analyze to determine what our most dangerous threats are. This can be difficult. Yet measured, carefully considered responses will be what secures this nation and its people.

In the last decade, the United States has been under an unprecedented attack. . In 2010, Department of Defense Deputy Under Secretary William Lynn said the theft of US intellectual property "may be the most significant cyberthreat that the United

---

[12] Lawfareblog, February 21, 2016, https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead.

[13] James Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," February 9, 2016, p. 1.

States will face over the long term."[14] The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. Make no mistake about it: this is an extremely serious national-security threat.

Protecting US intellectual property is critical for US economic and national security. In a July 2015 *Washington Post* op-ed, former NSA Director Mike McConnell, former DHS Secretary Michael Chertoff, and former Deputy Defense Secretary William Lynn concurred, observing that,

> Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interest … If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential."[15]

Messers Chertoff, McConnell, and Lynn concluded that the security provided by encrypted communications was more important than the difficulties encryption present to law enforcement.

As the Court noted in *Riley,*[16] the smartphones in our pockets are computers. They are, in fact, the most common device for accessing the network. So the cybersecurity threat applies as much to smartphones as it does to laptops, servers, and anything in between.

Securing Society

I'd like to turn now to encryption. I alluded earlier to NSA's efforts over the last two decades to secure private-sector telecommunications. Let me now present some detail.

Since the mid 1990s the NSA has actively been promoting the use of encryption in the private sector. This began with a 1995 incident in which NSA helped private-sector adoption of a new, more efficient cryptographic algorithm for securing low-powered, small devices.[17]

---

[14] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September/October 2010.

[15] Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, July 28, 2015.

[16] 134 S. Ct. 2473 (2014).

[17] An NSA representative present at an ANSI standards meeting spoke up to note that a new public-key cryptographic algorithm, whose security had been sharply questioned by the current provider of such algorithms, was in fact, secure. He said that it was sufficiently secure that the US government was adopting it for communications among all U.S. government agencies, including the Federal

NSA participated in the Advanced Encryption Standards (AES) effort by vetting submitted proposals. This algorithm was chosen through an international effort run by the National Institute of Standards and Technology, and is an extremely strong system. In November 2001, two months after the attacks of September 11th, NSA concurred in the approval of AES as a Federal Information Processing Standard (FIPS). Designation as a FIPS means an algorithm or protocol must be in systems sold to the U.S. government or contractors; such a designation increases industry and international acceptance.

A year and a half later, the NSA approved the use of AES to protect classified information as long as it was in an NSA-certified implementation.[18] The decision had great impact, for it vastly increases the market for products running the algorithm, thus ensuring wider availability for non-classified users as well. From there the NSA went on to approve a set of publicly available algorithms for securing a network.[19]

Why would the NSA go to such great efforts to support the deployment of strong cryptography in the private sector? Since the mid 1990s the Department of Defense (DoD) has relied on Commercial Off the Shelf (COTS) products for DoD communications and computer equipment. Use of COTS is required by law, but it is also good security practice. [20] The speed of innovation by industry means that DoD must use COTS products in order to be cutting edge. iPhones and iPads have been cleared for DoD use since 2013.[21]

This is not to say every soldier must carry a locked iPhone, but rather, on balance, the US government has had much to gain from the security improvements of private-sector communications technologies. It is thus no surprise that the NSA supported many of these, including the widespread use of strong encryption technologies.

Reserve. The result was that the algorithm was approved, and is now widely used. It was the first time anyone could recall the NSA endorsing a private-sector system in this way. See Ann Hibner Koblitz, Neal Koblitz & Alfred Menezes, "Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift," Journal of Number Theory, Vol. 131 (2011), pp. 781-814.

[18] Committee on National Security Systems, National Security Agency, Policy No. 15, Fact Sheet No. Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, 2003.

[19] Center for Secure Services, Information Assurance Directorate, National Security Agency, Suite B Algorithms, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (accessed by searching the archived copy of an older version of the website, available at: http://archive.today/mFaN)

[20] The Clinger-Cohen Act requires that DoD purchases of information technology use COTS whenever possible. See, more generally, Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

[21] Defense Information Systems Agency, "DISA Approves STIG for Government-Issued Apple iOS 6 Mobile Devices," May 17, 2013, http://www.disa.mil/News/PressResources/2013/STIG-Apple

Are We "Going Dark"?

Our hearing concerns whether the wiretapping world is actually "going dark." And here the story does not appear to be quite the way the FBI sees it. For although the FBI has been expressing great concern since the early 1990s that encryption would prevent law enforcement from wiretapping,[22] the sky has apparently not fallen—at least for the NSA.

In the wake of the San Bernardino shootings, the *Washington Post* reported that,

> Mike McConnell, who headed the NSA in the 1990s during the first national debate over federal encryption policy, recalled how 20 years ago, he was for back-door access to encrypted communications for the government.
>
> "NSA argued publicly, 'We're going deaf'" because of encrypted calls, said McConnell, who now serves on the board of several cybersecurity companies. The agency wanted a third party to hold a key to unlock coded calls. But the resulting outcry — similar to the one heard in today's debate over smartphone and text message encryption — caused the government to back down.
>
> "We lost," McConnell said simply. And what happened? "From that time until now, NSA has had better 'sigint' than any time in history," he said.[23]

Nor is Director McConnell an outlier in this view. In the same article, former NSA Director Michael Hayden[24] was quoted as saying that, "this is far more of a law enforcement issue than it is intelligence."[25] Hayden noted, "I'm not saying that NSA should not try to bust what Apple thinks is unbreakable encryption. All I'm saying is Apple should not be required" [to hold keys to decrypt data for the government].[26]

Now it is not surprising that some of the ex-NSA directors might hold this opinion. The NSA has two roles: signals intelligence and information assurance. The NSA has grown more concerned about the latter as the theft of US IP has reached

---

[22] In 1992 the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would no longer work: at least 40% would be intelligible and in the worst case all might be rendered useless (Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview, slide on Encryption Equipment," 1992. FOAIed document available at https://www.cs.columbia.edu/~smb/Telecommunications Overview 1992.pdf).

[23] Ellen Nakashima, "Former national security officials urge government to embrace rise of encryption," *Washington Post*, December 15, 2015.

[24] Director Michael Hayden was, also, of course Director of the CIA.

[25] Nakashima, "Former national security officials urge government to embrace rise of encryption," Ibid.

[26] Ibid.

astronomical levels. The FBI continues to remain focused on investigations rather than prevention—a very serious mistake, in my opinion.

The other reason for the split, of course, is that the NSA has far more resources and capabilities for conducting signals intelligence than law enforcement has. But that is exactly the point. In a technological world in which virtually every crime has a cyber component, the FBI needs technical expertise; it needs vastly more technical expertise than it has at present.

The Role of Smartphones

Not so long ago everyone in an important job with confidential information carried a Blackberry. This was the communication device of choice for those in high positions in government and the corporate world. Unlike the recent iPhones and Androids, Research in Motion, the manufacturer of Blackberrys, enables the phone's owner (the corporation for whom the user works) to have access to the unencrypted text of communications. If Syed Farook had been carrying a Blackberry,[27] there wouldn't be a break-into-the-phone issue.

But in the last decade Blackberrys lost popularity, losing the market to iPhones and Androids (that's because apps drive the smartphone business). Most people don't like to carry two devices. So instead of a Blackberry *and* an iPhone or Android, consumers choose to use a single consumer device for *all* their communications—and it happens to be a personal one. (Of course, that's not true for everyone. I am sure that many on this committee do carry two devices, one for government work, one for their personal stuff. People who work in the Department of Defense, or for defense contractors, the financial or other industries where keeping proprietary work data secure is crucial, may carry two devices.)

As a society we have largely moved to a world of BYOD (Bring Your Own Device) to work. And what that means is not only is your personal stuff—your notes and calendars and contacts—on your smartphone, so is proprietary information from work. And so access to US intellectual property lies not only on corporate servers —

---

[27] If the FBI had not asked the San Bernardino Health Department to reset the password on the phone's iCloud account, there would not be a break-into-the-phone issue (Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016). It is also the case that if the San Bernardino Health Department had installed "Mobile Device Management" on the phone it gave to Farook, there would not be a break-into-the-phone issue. (Tami Abdollah, "Apple CEO: Feds Should Withdraw Demand for iPhone Hack Help," ABC News, February 22, 2016, http://abcnews.go.com/Technology/wireStory/basic-software-held-key-shooters-iphone-unused-37106947)

which may or may not be well protected — but on millions of private communication devices.

Smartphones bear little relation to the simple rotary dial devices that once sat on hallway tables. Not only are smartphones the recipients of "our photos, our music, our notes, our calendars and contacts,"[28] much of it sensitive data (this is often especially true of photos). Our smartphones are used for conducting transactions of monetary value— ordering and paying for Uber rides and extra moves on Candy Crush, transferring balances between bank accounts, etc. People are also increasingly using their personal smartphones for business, and as a result, these smartphones store important proprietary information.

Smartphones are increasingly becoming wallets, providing access to accounts (not only financial, but also various online accounts, such as Dropbox), and storing emails and notes, including ones from meetings or design drawings and the like. For many people their personal smartphone acts as a convenient temporary repository for proprietary work information, information they know they ought to protect but rarely do as carefully as they ought. There are other ways of using phones for authentication; these rely on the device's security."

These smartphones are also used for authentication, that is, as a form of authentication to a device, an account, etc. And that means that the authentication information itself must be highly secured. Otherwise people in possession of the phone and with access to the data on it can break into other accounts. In short, smartphones are rapidly becoming a data repository of highly sensitive information, information that must be secured.

Thus Apple's secure by default provides an important improvement in security.

Smartphones and Long-Term Strategies for Security

Data theft through the Internet began three decades ago, starting with break-ins into military sites and the Defense Industrial Base.[29] As US companies began connecting their systems to the Internet, they, too, became targets. The scale of cyberexploition (data theft through networked systems) is what matters here. That scale is huge, and greatly worries General Alexander, Deputy Secretary Lynn, and many others in our government.

---

[28] Tim Cook, "A Message to Our Customers," February 16, 2016, https://www.apple.com/customer-letter/

[29] See, for example, Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace*, 1986-2012, CCSA Publication, 2013.

In the early days of the network, systems were poorly secured and data exfiltration was often the work of unsophisticated hackers. While aspects of that world still exist, the thieves are now far more sophisticated. Virtually every nation has its version of Cyber Command whose purpose includes spying via the network.

How do the spies get in? In a public presentation in January,[30] the Chief of NSA's Tailored Access Operations organization, Rob Joyce, observed that the most valuable data for attackers is your login credentials. Once an attacker has your login credentials—however briefly—he or she can establish a beachhead on your system that they can later use to exfiltrate data.

What has this got to do with securing phones? Everything. Using phones for secure login has the potential to rescue us from much of the mess created by the ease with which login credentials—typically passwords—are stolen. Currently our smartphones are our date books and our wallets, but they are well poised to become our authentication devices.

Smartphones already act as a "second factor" for authentication to accounts (e.g., Gmail); you log onto your email account with a password and an SMS to your phone provides a one-time PIN that you also type in. The security advantage is that someone needs two things to log into your account: your password and the SMS message.[31]

There are tremendous advantages to this approach. First, a smartphone is something you have, which makes it more secure than the "something you know" of a password. (The latter is easily used without your being aware that someone else has the authenticator—while you'd notice quickly that your phone is missing.) As Google explains, "It's an extra layer of security."[32] And a phone is something you already carry *all the time,* which means you're not carrying an extra device for authentication.

A Michigan start-up, Duo, provides two-factor authentication apps for companies that need fast, easy ways to ensure secure logins for their employees. Facebook is a good example. Its software engineers needed a *very secure* way to log on their development servers to write and submit code. The login process had to be fast—

---

[30] USENIX ENIGMA, https://www.youtube.com/watch?v=bDJb8WOJYdA, January 28, 2016.

[31] In fact, someone could intercept the SMS and, if they knew your password, log in instead of you. That would be a relatively highly targeted attack, meaning that Gmail's two-factor authentication system substantially improves on the more frequently used single factor of a password. There are other alternatives, including a "Security Key," that would be even stronger.

[32] Google, "Stronger Security for Your Google Account," https://www.google.com/landing/2step/#tab=how-it-protects.

and simple; programmers have little patience and will find workarounds if a process is complicated.[33]

There were various potential solutions: time-based tokens, one-time passwords, biometrics, smart cards and public keys. Each had serious problems,[34] and Facebook instead chose the Duo phone-based authentication solution for its developers.

Smartphones are used for security in other ways as well. Some of you have experienced Google's notification system that informs you about logins to your email account that are outside your normal behavior. The "Duo authentication feed" takes this security effort to a new level; it allows you to authenticate a transaction—for example, a login to an account—through a notification on your phone. You can respond while continuing your normal phone activity. This is security with convenience, meaning it is usable and effective security.

New technology means that smartphones are beginning to be used in even more creative ways to provide better security for authentication. This solves the problem that Rob Joyce says is his (and presumably other nations') most valuable way to gain access to your system.

Google is experimenting with a project where you log on by responding to a notification from a smartphone.[35] The holder of the smartphone gets the notification, responds, and then logs on to their account.

The private sector is not the only place using these approaches. Some high-placed agencies within the government are also adopting such solutions (and no, no details are available). Where security matters, authenticating through the device that is always in your pocket and owned by you is a much more secure way to handle your login credentials than the systems we've been using up until now.

If the information on the phone is accessible to Apple, it will be accessible to others—and this promising and important solution to protecting login credentials (which is, by NSA's description the most valuable way to break into systems)—will be ineffective. That's why locking down the data is so crucial for security. Rather than providing us with better security, the FBI's efforts will torpedo it.

---

[33] If only for this reason alone, security must be built in so that trusted but careless programmers don't make it easy to breach a system.

[34] Time-based tokens timed out when a developer was authenticating to two machines at once; one-time passwords had synchronization problems; biometrics are not trustworthy if the user is remote; and the smart card solution had interception problems. See: Facebook's Security Philosophy, and How Duo Helps, https://duo.com/assets/ebooks/Duo-Security-Facebook-Security-Philosophy.pdf

[35] Sarah Perez, "Google Begins Experimenting with Password-Free Logins," February 22, 2015, http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/

Securing the Smartphones Does Not Prevent Investigations

Even though Apple has engineered excellent security for the iPhone, there are workarounds to access the encrypted data that do not involve Apple creating an update that circumvents its security protections.

If a locked iPhone is brought to a WiFi network it knows, then the phone will automatically sync its contents with Apple's iCloud if the phone is charging and the phone and iCloud passwords match. Unfortunately the San Bernardino Health Department changed the iCloud password on Farook's phone the evening of the attack, and so the mismatching passwords (the ones on the iPhone and iCloud account) eliminated this potential solution. Synchronization won't occur if the passwords for the phone and iCloud account differ. The iCloud password reset was done at the behest of the FBI, which was concerned that someone else might try to access or otherwise affect the phone's iCloud backup.[36]

But there are other solutions.

There are, of course, lots of sites that discuss jailbreaking the phone.[37]

The Chaos Computer Club is a well established group of European hackers that has, for over thirty years, exposed security flaws in well-known systems. Their technical expertise is well respected. They ran a meeting last summer in which they demonstrated physical means, including the use of electron microscopes, to recover the data on security chips. Such techniques may well enable the recovery of the data on the iPhone, and would come cheap (as in well under fifty thousand dollars).

The security in the iPhone stems from the DMA chip, a piece of hardware that can access main memory without going through the CPU. The iPhone DMA is using AES; what the FBI really wants is the key. There are firms that do forensic work in "decapping" chips to expose information on them. Rough estimate of costs are around half a million dollars. I've heard other estimates that come in much lower, say in the one hundred thousand dollar range.

The point is that solutions to accessing the data *already exist within the forensic analysis community.*

There's another way of addressing the issue about whether Apple is impeding an investigation. That's to look at what information might be only be on the phone,

---

[36] Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016.

[37] Breaking into a locked iPhone would likely require technical skills at the level of a signals-intelligence agency.

keeping in mind that this phone was Farook's work phone and that he and Malik had destroyed their personal phones.

Let's start with might be only on the smartphone. There are likely to be text messages between Farook and his wife, there might be photos that Farook took of documents or people that might be of interest to the FBI, there might be communications between Farook and some of the Health Department employees he attacked.

Now I understand due diligence, and I especially understand due diligence in a terrorist attack that could conceivably have connections with other potential terrorists. But aside from self-professed statements in support of terrorist organizations, Farook and Malik do not appear to have been communicating with other terrorists. If they had been, the information about whom they are communicating with was available not only on their phones (personal or work), but also at the phone company and/or the ISP. (Farook might have been communicating via iMessage on his work phone. In that case, if the FBI made the request of Apple, they would have gotten iMessage metadata available from Apple servers.[38]) It is, however, extremely unlikely that Farook used his work phone rather than his personal one to conduct the private communications of interest.

Farook's communications with his coworkers are presumably available on their smartphones; one assumes these did not have passwords reset and their contents are accessible. It would thus appear that the only useful information that is potentially on Farook's smartphone is his communications with Malik.

In weighing the FBI request, one has to look at the potential gain and weigh it against the potential cost. In this case, the gain appears to be the possibility of developing a greater understanding of these self-radicalized terrorists.

The Security Risks Arising from Apple's Unlocking the Phone

Beginning with iOS 8, Apple iPhones encrypt by default, that is, all data on the smartphone is automatically encrypted unless the phone is unlocked. The key to unlock the phone data consists of an "entanglement" of the smartphone PIN and a hardware key physically embedded in the device. That means to get at the data, one has to have the phone. Apple's operating system protects the security of the data in other ways as well: with each incorrect guess of the phone PIN, the phone delays the

[38] The Manhattan DA report on smartphones notes that "iMessage detail (dates, times, phone numbers involved") does not appear at the phone company (Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, p. 12). That's correct. It is because an iMessage is an IP-based communication that goes through Apple servers.

time until the next guess is allowed. In addition, iOS may wipe the smartphone clean after too many incorrect tries. The system is designed to "protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it."[39]

Farook's work phone, an iPhone 5c, is an earlier device, but many of these protections are present on it as well. So at the FBI's request, the Central California District Court ordered Apple to create software that provides the FBI with:

> a Software Image File (SIF) that can be loaded onto [Farook's phone]. The SIF will load and run from Random Access Memory ("RAM") and will not modify the iOS on the actual phone, the user data partition or system partition on the device's flash memory. The SIF will be coded by Apple with a unique identifier of the phone so that the SIF would only load and execute on [Farook's phone]. The SIF will be loaded via Device Firmware Upgrade ("DFU") mode, recovery mode, or other applicable mode available to the FBI.[40]

The software is to:

> by-pass or disable the auto-erase function whether or not it has been enabled, … enable the FBI to submit passcodes to [Farook's phone] via the physical device port,[41] … and ensure that when the FBI submits passcodes to the [phone], software running on the device will not purposefully introduce any additional delay beyond what is incurred by Apple's hardware.[42]

In other words, the judge was asking Apple to create an Apple-signed device-specific software update tied to Farook's work phone.[43] The update would enable brute-force testing of PINs without erasing the content of the smartphone.

Let me briefly explain signing. Any complex digital device—a smartphone, a laptop, a thermostat, a car—will need software updates. Such updates are particularly important for patching newly discovered software vulnerabilities, but they have other functions as well. They provide new functionality (which means you don't need a new phone every six months). They also patch errors (all large software

---

[39] Apple Inc., *iOS Security: iOS 9.0 or Later*, September 2015, p. 4.

[40] United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.

[41] This would vastly speed up the time to try different PINs.

[42] Order Compelling Apple to Assist Agents in Search, p.2.

[43] Signing is a cryptographic operation that validates the authenticity of a digital object; in this case, it is that the code came from Apple.

systems have errors). And they keep complex digital systems working as the other systems around them change as they themselves are updated and improved.

In order to assure your device that the smartphone software update is coming from Apple, the company "signs" the update, employing a cryptographic process using information only Apple has. This enables a smartphone (or laptop, thermostat, car, etc.) to know that the update is coming from a legitimate provider and prevents malicious actors from presenting so-called "updates" to your machine that are actually attempts to install malware.

The FBI has argued that there is no security risk in Apple building and signing a device-specific software update tied to Farook's work phone. The update will be fully under Apple's control and will be tailored to work only on the smartphone in question.

These statements are both true and incorrect at the same time. That is, the FBI statements that the update will be under Apple's control and can be tied to work only on Farook's phone are factually correct. But they miss the point of the risks involved.

The fact is that the software cannot be developed, used, and deleted. Given that the phone's data may be used in investigations and court cases, the "break-in" software must remain available for examination. The longevity of the update code constitutes the first risk for Apple's iPhone users.

While the FBI affidavit says this is a one-time use, other cases make that highly unlikely. A November 2015 report from the Manhattan District Attorney's Office states that, "Between September 17, 2014 and October 1, 2015, the District Attorney's Office was unable to execute approximately 111 search warrants for smartphones."[44] Were Apple to develop the code that the FBI is requesting, shortly afterwards the company would be inundated with requests from state and local law enforcement for the same capability.

The frequent use that the code may be expected to have gives rise to the risk that Apple CEO Tim Cook described in a recent Q&A with the Apple employees:

> 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. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. Of course Apple would do our best to protect that key, but in a world where all of our data is

---

[44] Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf p. 9. The 111 phones were all running iOS 8.

> under constant threat, *it would be relentlessly attacked by hackers and cybercriminals*.[45] (emphasis added)

At present each OS and firmware update is signed by Apple, enabling an Apple device to recognize the proffered update is approved by Apple and not We-Break-into-You.com. This signing key ensures the integrity of Apple updates, but it seems very likely that US law enforcement will frequently want to search locked iPhones. Each search will be targeted to a particular phone, which means Apple must update the code to include the serial number of the target. Each particularized version of the code will need to be signed by Apple. That's where the risk arises.

Signing code is not technically hard. But a process that happens relatively rarely (e.g., when signing updates to the OS or firmware occur) is very different from the process for an event that occurs routinely (e.g., signing updates to accommodate frequent law-enforcement requests for access to the smartphones). Everyday use of signing updates to unlock smartphones means the signing process must become routinized. Though that doesn't sound like much of an issue, it actually presents a serious problem.

I am concerned that routinizing the signing process will make it too easy to subvert Apple's process and download malware onto customers' devices. My concern is not that the FBI will download rogue software updates onto unsuspecting customers; there is a rigorous wiretap warrant process to prevent government wiretaps from being abused. Rather I am concerned that routinization will make it too easy for a sophisticated enemy, whether organized crime or a nation attempting an Advanced Persistent Threat attack, to mislead the Apple signing process.

A process that is used rarely—such is now the case in signing updates—is a process that can be carefully scrutinized each time it occurs; the chance for malfeasance is low. But make things routine, and instead of several senior people being involved in the signing process, a web form is used, and a low-level employee is placed in charge of code signing. Scrutiny diminishes. No one pays a great deal of attention, and it becomes easy for rogue requests to be slipped into the queue.

All it takes for things to go badly wrong is a bit of neglect in the process or the collaboration of a rogue employee. And if the FBI, CIA, and NSA can suffer from rogue employees, then certainly Apple can as well. A phone that an unfriendly government, a criminal organization, or a business competitor wants to examine receives a signed security update from Apple. This enables the government, criminal group, or competitor to probe the smartphone and read its data when the

---

[45] Matthew Panzarino, "In Employee Email, Apple CEO Tim Cook Calls for Commission on Interaction of Technology and Intelligence Gathering," Techcrunch, February 22, 2016, http://techcrunch.com/2016/02/22/in-employee-email-apple-ceo-tim-cook-calls-for-commission-on-interaction-of-technology-and-intelligence-gathering/

smartphone is taken during a customs inspection, a theft, or a meeting in which all electronic devices are kept outside the room.

A different issue is that smartphone owners may begin to distrust the automatic update process. One of the greatest improvements to consumer device security has been automatic security updates, what we in the trade call a "push" instead of a "pull." Would people stop automatic updates if they were concerned that law enforcement were using the updates as a surreptitious technique to search their devices, not for terrorist activity but, say, for tax fraud?

Using updates that appear to have been signed by the company to deliver malware or surveillance technologies is likely to undermine one of the few success stories of cybersecurity: automatic updates to correct flaws. How many people would stop automatic smartphone updates from Apple if they knew that the update could steal their bank account information? How many people would stop using virus scanners on their PCs if they knew that these programs were sometimes used by law enforcement to spy on their users? If this activity were to cause people to back away from using automatic updates for patching and the like, the impact on security is likely to be disastrous.

Cryptography—and security technologies in general—protect data. Within that obvious statement lies a conundrum for the FBI. It would appear, that in its effort to use all tools to conduct investigations, the FBI has not fully considered the impact of its efforts on technologies that secure data (the lifeblood of the information economy).

There are potentially severe adverse cybersecurity consequences of the FBI approach. Apple has been carefully working to secure the data on customers' phones. Most security experts consider iOS to be the most secure platform—the last things we should be doing is seeking to weaken it. Were the District Court decision to be upheld, it will seriously undermine industry efforts in security. I don't doubt that Apple will continue to further engineering work to further secure the data on the smartphones[46] (and other devices), but the government's actions would give serious pause to other companies pursuing that direction.

International Impact of Forcing Apple to Unlock its Secured Phones

There are also serious international consequences that would stem from Apple's developing code to unsecure its iPhone's operating system. As I'm sure members of the committee are aware, when members of the US government and businesspeople

[46] Matt Apuzzo and Katie Benner, "Security 'Arms Race' as Apple Is Said to Harden iPhone," *New York Times*, February 25, 2016.

travel to certain countries, they bring "loaner" devices with them—phones and laptops that are wiped clean before they leave the US and wiped clean on return.[47] That's the case even though the devices never have their network connections turned on, at least by the owner. Recommendations for security include such steps as removing batteries from a phone when at meetings (in order to prevent a microphone being turned on remotely)[48] and keeping the device with you at all times.[49]

Apple's efforts to secure the data on the iPhone should be viewed in this light.

There is another international aspect to the FBI's efforts to unsecure the phone. United States support of human rights is a cornerstone of US foreign policy. It includes strong support for private and secure communications, for such capabilities are a necessity for human rights workers in repressive nations.

There is no question that authoritarian governments in such countries as Russia and China will demand Apple deliver the same software that is it has been ordered to develop to handle Farook's work phone.[50] Apple's ability to resist such demands is made much more difficult if it has already created the code for US government use.

Securing the iPhone follows in US government tradition of developing secure communication and data storage solutions for private-sector use. The US Naval Research Laboratories developed Tor, The Onion Router, an Internet-based tool for obscuring communications metadata (thus hiding who is communicating with whom). At first glance, this might seem counterproductive; after all, criminals hide their tracks that way. But Tor is also remarkably useful for the military (obscuring that personnel in safe houses are communicating with US command), for law-enforcement investigators (obscuring that a participant in a child porn chat room is actually an investigator from fbi.gov), enabling human-rights workers and journalists working in repressive regimes a modicum of safety, etc. Tor functions most effectively in protecting users' identities if more users are on the system (and if not all users are government employees).

Another project, one that has resonances with the iPhone, is a US Department of State Bureau of Democracy, Human Rights, and Labor supported program that

---

[47] Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," *New York Times*, February 20, 2012.

[48] Ibid.

[49] See, for example, North Dakota State University, "Cyber Security Tips for Traveling Abroad with Mobile Electronic Devices,"
https://www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/

[50] "And once developed for our government, it is only a matter of time before foreign governments demand the same tool." United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.

developed an information management tool, Martus.[51] Martus enables a group to create a searchable, encrypted database (say of human rights violations), and *this database provides access only to members of the group that created the account.* [52]

Given the threats to US businesspeople traveling overseas, and the strong interest and support of the US government to secure communication and data storage tools for human-rights workers abroad, the FBI stance makes no sense. If the FBI succeeds in having Apple develop software to unlock the phone, the bureau will, in effect, have provided our enemies with tools to use against us. But this is not the first time that the law enforcement has mistaken difficulties in conducting investigations with technology that must be changed to accommodate its needs. That approach mistakes where actual solutions should lie.

We Have Been Down this Route Before — and It is Dangerous

Five years ago I testified to a House Judiciary Subcommittee, the Subcommittee on Crime, Terrorism, and Homeland Security. At the time, FBI General Counsel Valerie Caproni expressed grave concern that due to encryption being used for communications (as opposed to for devices), the FBI was "going dark." At the time, the FBI sought to extend the *Communications Assistance for Law Enforcement Act* (CALEA) to Internet, or IP-based, communications.

Now CALEA is a very problematic law. Wiretapping is a way for an unauthorized third party to listen in to a communication. By requiring that wiretapping capabilities be built into telephone switches, the government created a security breach. Indeed there are many ways for nefarious sorts to take advantage of the opening afforded by law enforcement.

The story of the ten-month wiretapping of the cellphones of one hundred senior members of the Greek government including the Prime Minister, the heads of the ministries of national defense, foreign affairs, and justice is well known.[53] Less well known is the fact that an IBM researcher found multiple security problems in a Cisco architecture for the equivalent type of switch for wiretapping IP-based communications.[54] *But much more disturbing than either of these stories is the fact that when the NSA tested CALEA-compliant switches that had been submitted prior to*

---

[51] The Department of State supported deployment and training, particularly in Uganda and Zambia where LGBTQ activists use Martus for contact lists, testimonies, and similar information.

[52] "Martus 4.5: Strong Security, Easy Configuration, Enhanced Usability," https://benetech.org/2014/06/17/martus-4-5-strong-security-easy-configuration-enhanced-usability/ . Benetech does not hold the keys and could not decrypt the data if requested to.

[53] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, Vol. 44, No. 7 (July 2007), pp. 26-33.

[54] Tom Cross, "Exploiting Lawful Intercept to Wiretap the Internet," Black Hat DC 2010.

use in DoD systems, NSA found security problems in every single switch submitted for testing.[55]

CALEA did not apply to "information services," but in 2010, the FBI proposed that the law be extended to IP-based communications. As the world, knows, the Internet is remarkably insecure. Building wiretapping capabilities into switches and routers is a move that would make things substantively worse. And it is unnecessary, for there are other solutions that would provide law enforcement with the capabilities it needs without introducing new security flaws.

Many Internet communications, such as those using Google or Facebook services, are available to the companies in the clear. Thus, these communications services, while not falling precisely under the CALEA umbrella, remain easy for law enforcement to access (as indeed they have under court order).

Instead of requiring by law that communications systems be built "wiretap capable," it is possible to take advantage of the vulnerabilities of any large software system—and these include phones and computers—to install a remote wiretap.[56] Called "lawful hacking" because it is legal (done under a court order) and "hacking" because it involves hacking into the devices, is a method that has been successfully adopted by the FBI. In fact, it is an approach that has been used by the Bureau since at least 2001.[57]

The idea is simple—and relied on by attackers all the time. Using a wiretap warrant to probe a suspect's smartphone—or other communications device you wish to wiretap—and find a vulnerability on the device. Unfortunately such vulnerabilities are easy to find. Then law enforcement will need a second wiretap warrant to install the actual wiretap; the wiretap is installed by taking advantage of the vulnerability to download onto the device.[58]

Now this is an ugly sounding business, and indeed, civil libertarians have expressed concern about a wiretap solution that involves breaking into peoples' devices. But the fact is that if law enforcement is to continue to wiretap, it can do so either by

---

[55] Private communication with Richard George, Former Technical Director for Information Assurance, National Security Agency (Dec. 1, 2011).

[56] See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Going Bright: Wiretapping without Weakening Communications Infrastructure," *IEEE Security and Privacy*, Vol. 11, No. 1, January/February 2013, pp. 62-72 and also Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property,* Vol. 12, Issue 1, (2014).

[57] In the 2001 case, the FBI used software dubbed "Magic Lantern" to inject a virus into a remote computer and obtain the device's encryption keys. See B. Sullivan, "FBI Software Cracks Encryption Wall," NBC News, 20 Nov. 2001; www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall.

[58] This is the process by which criminals and other attackers download malware to extract data (of course, they do so without wiretap warrants).

taking advantage of vulnerabilities already present in the system to wiretap or by requiring all systems be made vulnerable (the CALEA solution). *Either you encourage security solutions that protect everyone by taking advantage of the security problems that already exist in the system, or you push everyone into less secure systems.* The former strengthens society's security while still enabling investigations; the latter only serves to weaken us badly.

A lawful hacking approach to wiretap investigations means that law enforcement must work a little harder.[59] Wiretapping investigations must be individually designed for each target (sometimes the same solution may work against more than one target). This is expensive, but that is not necessarily a bad thing; it means that we are not encouraging widespread wiretapping. I know that this is a value the Judiciary Committee holds dear.

The lawful hacking approach to wiretapping provides a roadmap for the locked smartphone situation.

Solutions for Locked Phones: FBI Investigatory Capabilities for the Twenty-first Century

Wiretap and search are extremely important tools for law enforcement, but encryption and locking down devices are extremely important security solutions for our data-driven, data-dependent society. But instead of embracing such technologies as an important and crucial security advance, law enforcement has largely seen such technologies as an impediment to lawfully authorized searches. This is a twentieth-century approach to a twenty-first century problem—but in that fact lies the possibility of a solution.

In the late 1990s, the NSA faced a similar crisis. Seymour Hersh detailed the situation in the *New Yorker*,

> The NSA, whose Cold War research into code breaking and electronic eavesdropping spurred the American computer revolution, has become a victim of the high-tech world it helped to create. Senior military and civilian bureaucrats … have failed to prepare fully for today's high-volume flow of E-mail and fibre-optic transmissions—even as nations throughout Europe, Asia, and the Third World have begun exchanging diplomatic and national-security messages encrypted in unbreakable digital code …[60]

---

[59] An NSA colleague once remarked to me that his agency had the right to break into certain systems, but no one ever guaranteed the right that it would be easy to do so.

[60] Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

As we all know, the NSA adapted.

The FBI is where the NSA was in 1999, and it has been there for quite some time (certainly since well before CALEA's passage).

Given the types of adversaries the US faces, and the skills they have, we should be strengthening and securing all forms of cyber, including those in consumer hands. That's exactly what Apple has done. We should be praising Apple for this direction, and at the same time, we should help law enforcement to adopt a twenty-first century approach.

The Bureau has some expertise in this direction, but it will need more, much more, both in numbers, but also in the depth.

The FBI will need an investigative center with agents with a deep technical understanding of modern telecommunications technologies; this means from the physical layer to the virtual one, and all the pieces in between. Since all phones are computers these days, this center will need to have the same level of deep expertise in computer science. In addition, there will need to be teams of researchers who understand various types of fielded devices. This will include not only where technology is and will be in six months, but where it may be in two to five years. This center will need to conduct research as to what new surveillance technologies will need to be developed as a result of the directions of new technologies. I am talking deep expertise here and strong capabilities, not light.

This expertise need not be in house. The FBI could pursue a solution in which they develop some of their own expertise and closely manage contractors to do some of the work. But however the Bureau pursues a solution, it must develop modern, state-of-the-art capabilities for surveillance.

Such capabilities will not come cheap, but the cost annually will be in the hundreds of millions, not in the billions. But given the alternatives—insecure communications technologies that preserve law-enforcement's ability to search and wiretap at the cost of enabling others to do so as well—the cost is something we not only can afford, but must.

Developing such capabilities will involve deep change for the Bureau, which remains agent based, not technology based. But just as the NSA had to change in the late 1990s, so must the FBI. In fact, that change is long overdue. As many in law enforcement have said, many if not most crimes now have a cyber component. The FBI must develop advanced capabilities for such investigations, moving to a technology based investigation agency. It is not there now.

Because of the complexity involved, state and local law enforcement will not be able to develop their own solutions for some, or perhaps many, cases. They will need to rely on outsiders, either contractors or an effort put together by the FBI.

It is neither the time nor place to exactly map out the full solution of how such a law-enforcement advanced technologies surveillance center will work. That will take the expertise of law enforcement, technical leaders, and Congress to study and determine. But I place this before you not only as a solution to the conundrum that Director Comey and District Attorney Vance present you, but as *the only solution that protects our security and enables law enforcement to do its job in the face of advanced communications technologies.*

What we as a nation, and you as lawmakers, need to do is enable the Bureau to develop that expertise and, also, to simultaneously determine the best way to develop structures to enable state and local law enforcement to take advantage of that expertise.

Encryption and other protections (such as time delays as incorrect PINs are entered) secure our systems, and should never be undermined. Instead, the FBI must learn to investigate smarter; you, Congress, can provide it with the resources and guidance to help it do so. Bring FBI investigative capabilities into the twenty-first century. That's what is needed here—and not undermining the best security that any consumer device has to date. For that's what Apple's iOS is.

Summing Up

Privacy is a deeply held human value; it is what enables us to laugh, to love, to tell embarrassing stories about ourselves, to take risks and expose ourselves, and to be deeply human. But while I care very deeply about privacy, I think that the business of securing communications and devices is ultimately a security versus security story, not a security versus privacy story.

We have become highly dependent on our devices for conducting all parts of our lives, and this will only expand in the future. But instead of going forward, for a moment I want to look back, quite far back. I want to end by noting what the preamble to the Constitution says,

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence [sic], promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Note that important phrase: "ensure the blessing of Liberty to ourselves and our Posterity." In the wake of the terrorist attacks in San Bernardino, it is easy to make a decision that argues in favor of short-term security by enabling this week's

investigation. It is much harder to make the decision that provides for long-term safety. But the preamble tells us to do so.

We have the option to press companies to develop as secure and private devices as they can, or to press them to go the other way. Let us make the right decision, for our safety, long-term security, and humanity.

Thank you.