Questions for the record from Chairman Bob Goodlatte (VA-06)

Responses from Susan Landau, Worcester Polytechnic Institute

1. You suggest in your testimony that "law enforcement must develop the capability for conducting such investigations themselves" and that Congress should provide appropriately funding for that endeavor. So, you do not object to the FBI's recently announced solution that enables access to the San Bernardino terrorist's phone?

Based on what's been publicly disclosed, such a solution is appropriate. There should also be two other aspects to this solution: a policy defining the process to determine when federal investigators should aid state and local law enforcement, who are unable to deploy sufficient resources to conduct such investigations (see response to question 13a) and policies to govern release of information about vulnerabilities to the manufacturers (see response to question 2).

2. At least one commentator has suggested that the FBI should now share its solution with Apple so that Apple can patch that particular vulnerability. Isn't that counterintuitive to your proposed solution to enable FBI to hack into phones without Apple's help. Doesn't it undermine FBI's efforts to share the solution with Apple who will only work to take away FBI's access to patching the vulnerability?

Two fundamental security needs are in conflict. One is the FBI's ability to examine phone contents during the course of an investigation; the other the ability of the phones' owners to secure data on the phones, which is crucial not just for the private information present on phones (such as photos, fitness information, and the like), but also because smartphones are increasingly functioning as security devices (that is, being used as authenticators).

Such conflicting security requirements are hardly new. For decades NSA's Signals Intelligence and Information Assurance Directorates had similar conflicts on precisely the issue of revealing security vulnerabilities in communications infrastructure. In NSA's case, resolutions partially depend on the extent of US reliance on the communications technology discovered to have a security flaw (the Vulnerabilities Equities Process is described at: https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities). Because the vast majority of FBI investigations occur in the US, vulnerabilities used by the Bureau are likely to also be present in devices used by many Americans. Sharing the vulnerability with the manufacturer enables faster patching of all phones with that vulnerability, and is important given the cybersecurity risks currently faced by the U.S.

Were the FBI to share the vulnerability information with Apple, there would be a window of opportunity before the vulnerability was actually patched. During that time, the FBI could continue to use the vulnerability on other phones.

3. Would you say that the work-around solution that FBI has founds is safe in the hands of the FBI?

It appears that the FBI has not learned the details of how the vulnerability works, so yes it is (the Bureau can't reveal information it doesn't know). The fact that the vulnerability exists, however, means that others, including signals intelligence organizations of nation states and organized crime, will look for it, and, with time, undoubtedly find it. This could occur through discovery, or through theft or purchase.

4. Why does it matter whether the FBI possesses the internal capabilities to decrypt a device or communication or the provider possesses it? Wouldn't it be equally vulnerable to cyber hackers and criminals or enemy nations?

By requesting that Apple develop third-party access to a secured device, the FBI was effectively asking to create a weakness in the security system protecting iPhone 5cs. As we learned during the House Judiciary Committee testimony on March 1, had this capability been developed, it would have been frequently used by law enforcement agents around the country. Such routine use would substantively increase the risk that the iPhone security system would be subverted through rogue requests submitted to Apple. (Note that I am not suggesting that law enforcement would be submitting rogue requests. My concern is that other groups, including organized crime and other nations, would subvert the necessarily routine process needed to service the thousands of requests that would come in annually.) The capabilities Apple would have to develop would have increased the risk of insider attack as well as theft of the code from the company.

Were Apple to have developed such software, *all* iPhone 5cs would have been at risk (and perhaps other iPhones as well; that depends on platform-specific architecture). In addition, were Apple to have developed the software to decrypt a device or communication, that capability would be demanded by law enforcement of other nations, including those that fail to respect the rule of law.

5. What recourse does an employer have to get information from either a phone it owns but is used by an employee or a phone owned by an employee for work purposes, especially if all the employee has to do is not backup the phone?

Mobile Device Management systems (MDMs) can be implemented on work phones used by an employee and personal phones used by an employee for work-related tasks. Many vendors support MDM and many enterprises configure it, but it is not automatic; it must be deliberately configured. Use of an MDM arrangement is

elective on the part of the employer, but not all employers implement the system sufficiently well for it to work completely.

There are many types of MDMs offered by a variety of providers, and they function differently. Furthermore, contracts between the employer and user can change, and even a single provider's MDM arrangement can change in the future. Thus it is impossible to give a definitive answer to this question.

A partial answer is supplied by the fact that MDMs typically enable the phone's owner to wipe the phone, which means that a non-compliant employee (e.g., an employee who is not backing up their phone) risks losing all the data on their phone, including personal information stored on the device. This provides a strong incentive for backing up the phone according to the employer's requirements.

6. You have discussed how the Apple iPhone uses hardware encryption embedded on a physical chip. One recent story on Google also suggested that it is reviewing hardware-based encryption stored on individual chips. In layman's terms, can you explain the difference between hardware encryption and software encryption?

For the purpose of this question, "hardware encryption" means the encryption in an isolated piece of hardware (typically a chip). The encryption process and all its data are kept within what NSA calls a ``cryptographic boundary'' that prevents a compromise of the surrounding computer environment, particularly the operating system, from extracting data from the cryptographic processor by any means other than those the processor provides.

The reason that hardware encryption is viewed as potentially more secure than a software solution is that you can reprogram software, but swapping out the hardware is more difficult. And in hardware solutions, part of the key resides in hardware, meaning it cannot be retrieved by software.

7. In your testimony, you suggested that a locked phone can simply be brought into a Wi-Fi network and as long as the passcode and iTunes password match and the phone is charging, then the contents of the phone will sync to the iCloud. Then law enforcement can simply issue a search warrant for the what's in the cloud.

a. Why is the cloud so much more optimal a place for law enforcement to seek communications and associated data?

Data on the iCloud is encrypted by Apple, which holds the decryption key. (While users could encrypt data before saving it in the iCloud, there is no default option to do so—and no way to do it for standard iOS applications.) This means that Apple has the capability to access the data in unencrypted form, and thus so can law enforcement under court order.

b. Is it so much more secure than the phone that it can be both encrypted and accessible at the same time?

As a security measure, the iCloud data is encrypted. However, as noted, the iCloud encryption keys are held by Apple. This means that the data is accessible to Apple in unencrypted form.

If so, why isn't the technology used to run the cloud sufficient to protect the device?

There is a lot of information on phones that is not, and should not, be shared. The usual issue of concern is personal information— photos, private communications, etc. But from a security vantage point, the most important information on a phone is authentication information. Phones are being used to authenticate users to their online accounts of various sorts: email, financial, etc. Such authentication information should not leave the device except when authenticating the user to the account. Any requirement that all data on the phones be shared with a cloud provider would eliminate the ability of phones to serve as secure authenticators.

c. What about a remote-erase command? Wouldn't that kick in as soon as the phone is connected to Wi-Fi and charging?

That command could be disabled on the iCloud end on a per-user basis. This isn't that hard, since it is already possible to do so on a per-phone option.

8. If the forensics community already possesses solutions to accessing the data on an encrypted iPhone, doesn't that mean that even the end-to-end encryption can be circumvented?

Yes, there are many ways that the end-to-end encryption can be circumvented. One way can be because the actual system providing end-to-end encryption has a security flaw that thus enables wiretapping clear text after all. A second way is if wiretapping capability is downloaded on the phone. Even though the conversation itself is encrypted end-to-end, it is available at the phone in unencrypted form. Thus a wiretap on the phone can capture the communications content. Finally, if one has physical possession of the device, it is possible to download a wiretap onto the phone.

It is possible to download a wiretap onto a device through security flaws in either other applications on the phone or the phone's operating system; see my paper with Steven Bellovin, Matt Blaze, and Sandy Clark, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip. The key issue is that all complex systems, even ones architected to

be secure, contain vulnerabilities. As we all know, hackers, not Apple, ultimately enabled the unlocking of Farook's phone.

And if that's the case, then why should the government look to hackers instead of Apple to unlock the phone?

Hackers and Apple have very different motivations. Hackers who sell vulnerabilities are interested in prolonging the use of a vulnerability, while Apple's interest is in patching the security flaw as quickly as possible. We want to encourage that behavior in Apple—rather than encouraging the company to make poorly secured devices, which would leave the phone open to criminal hackers and spies.

9. If Congress enacts specific legislation to require device manufacturers and app designers to decrypt and unlock their technologies, isn't this incentive for foreign manufacturers to market products with stronger encryption than U.S. products? And couldn't this drive U.S. consumers to those foreign products, thus creating an even greater barrier for U.S. law enforcement?

Yes, and this is a strong argument that such legislation would harm U.S. manufacturers. It would also decrease the ability of U.S. law enforcement to get the information

This aspect of the problem is a replay of the situation in the 1990s and is part of the reason for the loosened export controls that came into play in 2000. Note that it will be impossible to regulate software deployment; we are not going to have US Customs check which apps are on a phone as people enter the United States.

We could regulate hardware by requiring that hardware encryption enable third-party access. But one, there is no simple solution from a technical vantage point (see some of the problems with split keys in response to question 11). And more importantly, weakening hardware security through requiring an access point means that smartphones cannot be trusted as secure authenticators. This would severely limit strong security solutions, *including those used by the US federal government.*

10. Even though the FBI has now been successful in bypassing the auto-erase functions of Farook's iPhone, that does not mean that all of the information stored on the phone will automatically become available to them, correct? Encrypted apps on the phone will still have to be separately accessed?

It depends on how the apps have been designed and whether logging into the phone also logs into the app, or whether a separate login is needed for the application.

11. The Director of the NSA has called for the use of "split keys" as a potential solution. Could you describe in layman's terms what is meant by "split keys" and whether such an option is workable in your opinion?

There are many versions of "split keys," but basically they are solutions in which the encryption key is split in a number of parts, say *n*, and some portion of them, *m*—where *m* can be smaller than *n*—are needed to recover the encrypted information (examples are 2or 3 split keys out of a possible 3; 2, 3, or 4 out of a possible 4; 2, 3, 4, or 5 out of possible 5; etc.).

There are serious problems with such a solution. A solution with few keyholders—a half dozen governments and as many companies—suffers from the "trust" issue; why should one government trust a system in which other governments, but not themselves, hold the keys. But if there are many keyholders—hundreds of governments, thousands of companies—it becomes impossible to secure the keys.

In other words, the split-key solution sounds good in theory, but collapses as soon as one begins to examine the details of how it would actually work in practice.

12. Is it possible for a bad actor to modify encryption or gain access to encryption keys?

Yes. There are many examples of this. The most recent—and very serious—one was a compromise of the Juniper VPN, which was done by replacing a parameter that generates random key bits. This vulnerability allowed attackers to monitor VPN traffic. See "On the Juniper backdoor" by Matt Green, http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html, for details on the attack.

13. You have been critical of solutions that involved updating CALEA because doing so, you argue, would only serve to increase security vulnerabilities. If we rely solely on the FBI's ability to create ad hoc solutions to surveillance or access problems, are we not also ensuring that law enforcement is always playing catch-up with criminals and national security threats when time is of the essence?

As we understand all too well, our society has become remarkably dependent on an insecure electronic communications infrastructure for both the control of critical infrastructure and for conducting business. The latter means not just selling items on eBay, but managing a globalized industrial manufacturing base, just-in-time inventory, remote work, etc. This is the context for the Apple/FBI iPhone case, and for the larger discussion of investigations involving secured electronic communications and devices.

Thus the answer to the question is both yes and no. The FBI needs to develop an investigative center with agents with a deep technical understanding of modern telecommunications technologies which will include capabilities of understanding not only where technology is and will be in six months, but where it may be in two to five years. Sometimes the FBI will be ahead of criminals and national-security threats, but, as the NSA well knows, it cannot always be ahead. Sometimes it will

have to play catch up. One of the important advantages of our highly interconnected electronic world is that even if playing catch up in decrypting texts or opening devices, the FBI will have a wealth of other electronic trails to follow as well.

a. If the FBI can't stay ahead of encryption technology, how do you suggest state and locals have the capability to do so?

State and local investigators already lack the technical expertise to investigate the multiple different types of cellphones, and this will only get worse with time and increasing complexity. Given the myriad number of communications technologies and the rapid rate of their innovation, it makes sense to fund a central source for solutions, and to develop a policy that determines the criteria for sharing those solutions. It will not be possible to develop solutions for all devices and all applications, but making choices about which cases to pursue and what resources to devote to them has always been part of law enforcement's task.

Congress should consider what the appropriate policy mechanism is for determining when to share electronic surveillance technologies; such decisions should not be made by the organization that actually does the work.

14. To pose a hypothetical: What if terrorists are currently planning a 9/11-like attack and storing their plans on encrypted phones? If any of the those phones were to be captured either before or after an attack, do you believe that the manufacturer of those phones should ever have a legal duty to provide the government access to content and metadata stored on the phones?

This hypothetical needs to take into account the various risks facing the US. So the issue is whether it is possible to provide such a capability without simultaneously creating serious holes that others can exploit.

Up until now the capabilities for serious cyberattacks have been limited to nations that have motivations *not* to attack the US in this way. But the situation is changing, and increasingly other nations have developed greater capabilities for cyberattack. With that change, the need to prevent creating serious holes that others can exploit increases.

15. Isn't preventing the United States government from lawfully accessing encrypted communications pursuant to a court order or search warrant based on probable cause fundamentally different than turning over the same information to hostile regimes or those foreign governments that do not respect the rule of law?

Yes, but this phrasing of the question doesn't adequately capture the issues faced by phone manufacturers. While U.S. government access pursuant to a court order is different legally from requirements by hostile regimes or foreign governments that do not respect the rule of law to turn over the same information, its practical consequences are the same. It is much easier for a vendor to say "no" to a totalitarian government if the vendor isn't capable of complying than if they have the capability but do not want to exercise it on that government's behalf.