Before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

Testimony of Daniel J. Weitzner, Director
MIT Internet Policy Research Initiative
Principal Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory

Hearing on "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives" -- April 19, 2016

Summary

While recognizing the legitimate needs of law enforcement and challenges raised by increasing widespread encryption, there is now a well-developed consensus among policy-makers and computer security experts that mandating infrastructure-wide back doors is the wrong approach to dealing with the complex intersection of public safety, network security and individual privacy needs. As Congress addresses this important issue, there are several cautions to observe, as well as affirmative steps that can identify positive paths forward. Scientific investigation of current computer security challenges teaches that the last thing policymakers should do is to cause new vulnerabilities to be introduced into the global Internet and mobile device infrastructure. We must also be careful to avoid any new disincentives that would discourage the best possible technical security architectures from being deployed. The challenge of keeping our information infrastructure secure is already so great. We must not put new stumbling blocks in the way.

There will be a temptation to look for a 'one size, fits all' regulatory answer to the complex question before us. The Communications Assistance for Law Enforcement Act (CALEA) was a reasonable way to address surveillance obligations of high-regulated, centralized, national telecommunications companies. However, the highly diverse, global and decentralized firms that make up the Internet platform and mobile industries are a poor for for this top-down regulatory model. Instead, Congress can find constructive paths forward with careful analysis of specific cases in which law enforcement faces roadblocks, and recognition that any surveillance requirements imposed by courts or legislatures have to scale up to hundreds or thousands of providers. Finally, increased transparency and privacy protection under law will help assure the public that surveillance authorities are subject to effective accountability, committed to respect for user privacy and protection of the underlying security of the global information infrastructure.

Introduction

Thank you Chairman Murphy and Ranking Member DeGette, for inviting me to appear before you at this hearing on encryption, surveillance and privacy. My name is Daniel J. Weitzner. I am Founding Director of the MIT Internet Policy Research Initiative and Principal Research Scientist at the MIT Computer Science and Artificial Intelligence Lab. From 2011-2012, I was United States Deputy Chief Technology Officer for Internet Policy in the White House. My computer science research includes the development of Accountable Systems architecture to enable computational treatment of legal rules and automated compliance auditing. I teach Internet public policy in MIT's Electrical Engineering and Computer Science Department. Before joining MIT in 1998, I was founder and Deputy Director of the Center for Democracy and Technology, and Deputy Policy Director of the Electronic Frontier Foundation.

I. Phase One of the Debate is Over - Infrastructure-wide back doors are a bad idea

This hearing comes at an important time in the broad debate about how best to accommodate law enforcement's legitimate needs for investigative access to Internet platforms, mobile devices and apps. Some in the law enforcement community have suggested that mandating infrastructure-wide back doors would be a reasonable way to meet law enforcement needs. And they hoped that there would be a way to do this without unreasonable security risk. No one should doubt that law enforcement investigators face real challenges in the digital world as a result of the easy availability of strong encryption. Still, even those who are most sympathetic to law enforcement needs are joining the consensus view that infrastructure-wide back doors are too risky to implement. Therefore, the debate is shifting from looking for a "one-size, fits all" solution to a more nuanced assessment of how to address the complex challenges faced by law enforcement while supported continued strengthening of Internet security measures.

Following initial calls from FBI Director James Comey and UK Prime Minister David Cameron for infrastructure-wide back doors, a group of cryptographers and computer security experts came together to evaluate the technical security impact of such an approach. We found that mandatory, infrastructure-wide exceptional access would cause three fundamental problems. First, providing exceptional access to communications would force a U-turn from the best

practices now being deployed to make the Internet more secure.[1] These practices include forward secrecy—where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security—every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. One might hope that the encryption problem could be 'solved' with a single, top-down approach much as CALEA did for traditional telecommunications systems. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious—making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple key holders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the U.S. Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data

[1] Keys under doormats: mandating insecurity by requiring government access to all data and communications. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze,Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J.Weitzner
Journal of Cybersecurity Nov 2015.
http://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009.full

because OPM had insecure infrastructure. If service providers implement exceptional access requirements incorrectly, the security of all of their users will be at risk.

In response to these arguments and related views from computer security experts around the world, the new phase of the debate is characterized by a growing acceptance that mandatory, infrastructure-wide back doors are a bad idea. In the more than six months since our article was first published in a peer-reviewed journal, we have only been able to find one academic computer scientist who has questioned our finding.[2] In a blog post, a well-respected Dutch computer security researcher accepted most of our arguments but indicated that we had not proved that it is absolutely impossible to build secure exceptional access systems. Still, he implicitly agreed with our stated view that it is very hard and therefore very risky.

Political leaders from around the world are now publicly rejecting the idea of mandatory back doors. Recently, US Secretary of Defense Ash Carter offered his view at the RSA Conference:

> As we together engineer approaches to overall human security in the information age, I know enough to recognize that there will not be some simple, overall technical solution—a so-called 'back door' that does it all…. I'm not a believer in backdoors or a single technical approach. I don't think that's realistic.

Last month, Robert Hannigan, Director of the UK's GCHQ (the lead UK government surveillance agency) gave a talk at MIT—entitled "Front Doors and Strong Locks: Encryption, Privacy and Intelligence Gathering in the Digital Era"[3]—on his views of the evolving issues of encryption and surveillance. His message was clear: It does not make sense to ban or weaken end-to-end-encryption, nor does he favor 'backdoors' in the infrastructure. But he believes the obstacles posed by encryption are a "moral challenge" that society, broadly speaking, must face. Hannigan's emphasis on GCHQ's information assurance mission makes clear that companies should only be required to offer assistance in a manner that avoids creating security risks. As he says,

---

[2] The second crypto war is not about crypto, Jaap-Henk Hoepman. https://www.cqure.nl/kennisplatform/the-second-crypto-war-is-not-about-crypto

[3] http://www.gchq.gov.uk/press_and_media/speeches/Pages/hannigan-speech-at-mit-front-doors-and-strong-locks.aspx

> Much of GCHQ's work is on cyber security, and given the industrial-scale theft of intellectual property from our companies and universities, I'm acutely aware of the importance of promoting strong protections in general, and strong encryption in particular. The stakes are high and they are not all about counter terrorism.

Adding that he is "accountable to our Prime Minister just as much, if not more, for the state of cyber security in the UK as I am for intelligence collection," he is outright opposed to mandatory back doors:

> The solution is not, of course, that encryption should be weakened, let alone banned. But neither is it true that nothing can be done without weakening encryption. I am not in favour of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors.

Speaking[4] with US Secretary of Commerce Penny Pritzker, European Commission Vice President Anders Ansip repeated his opposition to weakening encryption with mandatory back doors. Ansip argued that people simply will not trust systems that have built-in governmental controls. Drawing from his experience as the Prime Minister of Estonia who famously digitized much of the government, he observed that over two-thirds of Estonian citizens vote online. "How will they trust the results of the election," VP Ansip asked, " if they know that the government has a back door into the technology used to collect citizen's votes?"

These statements from US, UK and EU government officials demonstrate that our underlying technical analysis against mandatory back doors in Keys Under Doormats has been largely accepted.

II. Cautions going forward

The debate has moved beyond the false, binary choice that would have us either aim to guarantee the success of all law enforcement surveillance requests, and ignore the broader security impact, or at the other extreme, simply declare that law enforcement is entirely on its

[4] http://webcast.amps.ms.mit.edu/spr2016/DOC/1610/5.html

own in the age of strong encryption. Moving forward, how should policymakers address the important interests of law enforcement, security, privacy and global competitiveness? It will remain important to avoid mandating technical security vulnerabilities as even small security gaps can spread and cause widespread damage. And we must avoid creating undue burdens on efforts to make our infrastructure more secure, so we can meet challenge of designing and maintaining our global information infrastructure with strong confidentiality, resilience, and reliability.

A. Avoid mandating technical security vulnerabilities that can easily propagate throughout the entire global Internet infrastructure

Some law enforcement arguments calling for exceptional access suggest that that Apple and Google's increased focus on encryption is not actually about increasing the security of the device; that this push is a marketing ploy for privacy conscious users in the post-Snowden era. Mobile devices appeared to function perfectly well before the switch to full disk encryption, so why change now?

The history of computer security shows that the push to ubiquitous encryption is well motivated by the litany of systemic vulnerabilities resulting from hardware and software vendors failing to encrypt and/or cryptographically verify data. Further, the damage from failures to properly encrypt data has historically been exacerbated by the slow and arduous pace of eliminating bad code once it has been added to the overall software ecosystem. The combination of these two factors has led the security community to advocate for applying encryption and authentication to as much as is possible, since failing to do so has been repeatedly shown to cause serious damage to user security and privacy.

One of the points of contention between Apple and the FBI in the San Bernardino case is whether Apple can be compelled to 'sign' a new version of the Apple iOS operating system whose function is to enable law enforcement access to the locked phone. Code-signing is an important security technique that prevents malicious software from running on a user's device. Before the FBI found an alternative method to break into the phone, they sought a court order to force Apple to sign the code, thereby enabling that version of iOS to run on the seized phone. Apple users rely on the company to only sign code that is safe for use. While Apple's refusal to agree to sign a weakened version of iOS was a stumbling block for the FBI, it is also a means of

protecting the integrity of the code-signing mechanism is essential to the security of all iPhone users. Failing to cryptographically verify updates through this code signing process can lead to developer's software being subverted to spread malware. Flame, a sophisticated nation-state malware campaign discovered in 2012, exploited Microsoft Update's outdated cryptography to infect Windows PCs.[5] Apple failing to cryptographically verify updates to iTunes turned the program into an infection point for the FinFisher virus,[6] which was then found to be in use by oppressive governments spying on local dissidents.[7][8] Most recently, an update framework used by hundreds of OS X apps was found to be vulnerable to these exact same sorts of attacks, leaving thousands of users at risk of losing complete control of their computers, including anything they access on that device --- bank accounts, private chat, email accounts, health records, and social media.[9]

Another class of attacks involve the interception of account information from websites or apps that do not encrypt their data in transit. For instance, as recently as 2010, major websites including Facebook, Google, Linkedin, and Reddit failed to encrypt connections to their sites using HTTP over the TLS/SSL secure transport protocols, known as HTTPS. This failure made those sites vulnerable to "session hijacking attacks" that allowed attackers watching the network to gain access to user accounts. Such attacks were not difficult to execute, for instance, an easily installable Firefox plugin called Firesheep allowed anyone in the vicinity of an unencrypted wifi connection to gain access to unsuspecting users' email, social media, and bank accounts with a literal click of a button.[10] To see how far-reaching this vulnerability could be, think of all the times users connect to an untrusted airport wifi hotspot to download an app, to check email, access health records, or converse with friends. Strong encryption makes it possible for that user to do so without needing to fully trust the myriad of devices and organizations between his or her device and the service being accessed. Conversely, without encryption, a malicious middleman such as the wifi router owner, the Internet service provider, or a disgruntled network administrator could easily gain control of an unsuspecting user's computer or bank account.

---

[5] http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate/

[6] http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/

[7] http://www.bbc.com/news/uk-34529237

[8] http://bits.blogs.nytimes.com/2012/08/13/elusive-finspy-spyware-pops-up-in-10-countries/

[9] https://vulnsec.com/2016/osx-apps-vulnerabilities/

[10] The tool, called Firesheep, allowed amateur attackers to gain surreptitious access to unsuspecting users' Facebook, Reddit, Gmail, Yahoo, and Twitter accounts. http://codebutler.com/firesheep/

Computer security architects are inclined to advocate the widest possible deployment of cryptography in the infrastructure because it is impossible possible to know in advance what applications and services will require strong security or how the threats may evolve. For instance, even a few years ago, code signing, full-disk encryption, and HTTPS were viewed as tools only for high-security applications. Today, any company that did not use code signing for software updates, HTTPS for their ecommerce websites, or full-disk encryption for their employee laptops would be compromised in short order.

Inadequate computer security design choices, like absent or out-of-date cryptography, stick around for a long time and are hard to clean up once deployed in the infrastructure. The Flame virus infection vector, cited above, was caused by Microsoft's use of an outdated cryptographic primitive that had been shown to be flawed more than five years before.[11] Even when developers produce patches for bad crypto, users might not switch over for compatibility reasons --- the TJ Maxx intrusion, which cost that company upward of $250 million, was caused by their use of a woefully outdated encryption scheme (WEP) on one of the company's wifi access points. Finally, a 2013 study by the University of Michigan found that tens of thousands of websites were using outdated cryptographic primitives such as weak keys and other easily avoidable misconfigurations.[12]

It follows that one of the major concerns with exceptional access capabilities is that the bugs they inevitably introduce will be difficult to fix. It is important to note that this is not a theoretical problem: Past forays into regulation mandating weakened encryption for foreign export during the early 90s, so-called "export-grade encryption," resulted in the 2015 FREAK class of vulnerabilities, which in turn led to roughly 12% of the top million most visited websites being interceptable, including usajobs.gov and americanexpress.com. FREAK worked because a malicious middleman could force the use of weak export grade cryptography in cases where both the browser and the server happened to still support the outdated protocol,[13] which had unfortunately been kept around for backward compatibility even after the export cryptography regulation had been lifted.

[11] The first known practical break of md5 happened in 2005, and Flame was found in 2012. http://eprint.iacr.org/2005/067

[12] https://jhalderm.com/pub/papers/https-imc13.pdf

[13] See FREAK and DROWN (https://freakattack.com/, https://drownattack.com/)

The damage caused by flaws in cryptographic implementations is compounded by the fact that these cryptographic systems are extraordinarily interdependent at the operating system and application level. Writing good crypto code is difficult. Correct implementation of cryptographic algorithms requires deep theoretical computer science and systems-level knowledge, applications almost always rely on third-party libraries or services to encrypt both data at rest and in transit. In fact, the difficulty in implementing cryptography has led to very few implementations of these frameworks; for instance, almost every Android device uses one of two libraries.[14] Bugs introduced in such cryptographic frameworks (like Android's libraries) would therefore proliferate to vulnerabilities in seemingly unrelated apps (like your banking or email app).

These factors show that vulnerabilities introduced by weakening encryption, including mandating exceptional access, will propagate widely and could cause widespread, hard-to-measure damage. Vulnerabilities introduced by weakening encryption, including mandating exceptional access, will propagate to a wide range of security-critical applications. Therefore mandating exceptional access or other system-wide vulnerabilities is tantamount to mandating chronically vulnerable devices and services.

B. Avoid introducing disincentives to using secure systems development practices

Any proposed regulation on encryption must take into account the chilling effect on adoption and continued use of good security procedures. Incentivizing good security is already quite hard. Today, though cryptography is relatively unfettered by regulation, there are nonetheless disincentives for businesses to properly secure their users' data. It would be reasonable to assume that adding more disincentives would risk causing the rapid abandonment of these otherwise beneficial security procedures.

The difficulty of using cryptographic tools both in development and by end-users are well known in computer security research. A 2013 study of the Google Play app store found that, of 11,748 different applications tested, only 1,421 (12%) made correct use of the cryptographic libraries available, leaving many apps vulnerable to known bugs.[15] Users have encountered similar

[14] A great paper on the state of cryptography on Android is "An Empirical Study of Cryptographic Misuse in Android Applications" by Egele et al. Indeed, the paper finds that the vast majority of app developers fail to use these libraries properly. https://www.cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

[15] https://www.cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

difficulties, often making it rational to ignore encryption and security advice in order to more easily complete daily goals.[16]

In addition to user and developer and user error, device manufacturers must deal with physical limitations --- battery life and processing speed can be drastically affected by the use of encryption, which is only ameliorated by use of specialized, currently more expensive hardware. Google, for instance, backed away from forcing full disk encryption on all devices citing battery life and usability as concerns.[17]

Regulation will compound the above disincentives. Imagine a burgeoning tech startup deciding whether or not to spend the time and capital to properly encrypt their services, or to encrypt their data at rest. Without having to worry about compliance, the company's choice is somewhat straightforward --- it will be more likely to bake security in from day one since a high-profile failure will damage their brand. However, with regulation, that same company runs a risk of accidentally running afoul of government-mandated of exceptional access requirements.

Amazon, far from a struggling firm, recently decided to remove full-disk encryption from their Kindle Fire, almost immediately after the FBI brought suit against Apple in San Bernardino.[18] It is unimportant whether such concessions are due to fear of government lawsuits or the technical issues --- either way they demonstrate that even the best-resourced companies have competing incentives about implementing full-disk encryption on their devices.

C. Avoid top-down regulatory approaches - they are likely to fail in the global Internet environment

As this Committee considers how to address the very real needs of federal, state and local law enforcement to conduct investigations in the digital environment, examination of existing regulatory models in the law of electronic surveillance can be helpful in identifying models to adopt and models to avoid. As a case in point, there have been calls over the last several years calls[19] to address this difficult question by simply extending the Communications Assistance for

[16] http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf
[17] http://www.theverge.com/2015/3/3/8143607/android-lollipop-default-disk-encryption-performance
[18] http://motherboard.vice.com/read/amazon-removes-device-encryption-fire-os-kindle-phones-and-tablets
[19] http://www.cnet.com/news/fbi-to-announce-new-net-wiretapping-push/

Law Enforcement Act (CALEA)[20] to apply to Internet companies. But close examination of CALEA in the context of today's digital surveillance challenges shows just how hard it would be "solve" these problems with the top-down regulatory approach used in CALEA. CALEA was drafted to address the conduct of a very small number of traditional telecommunications companies all of which were subject to (then) stable and well-understood regulatory authority of the FCC. No such regulatory control exists for the Internet and mobile industries. The companies under CALEA's purview are all mature, US-based companies with slowly-evolving products largely focused on the domestic marketplace. By contrast, the services at the heart of the FBI's challenge today are rapidly evolving in scale, scope and location in the world. Finally, while CALEA's regulatory structure is complex, its goal is simple - preserve status quo surveillance capability. The deep uncertainty about the constitutional scope of surveillance authority in the Internet and mobile environment as a result of rapid evolution in new services means that drafters of a new law would have no stable surveillance goal around which to build a statute.

First, CALEA targeted the behavior of the traditional telecommunications industry, which was already regulated by Congress under the Communications Act under the Federal Communications Commission. Companies providing the telecommunications services regulated by CALEA had a clearly defined relationship with the regulatory agency so legislative drafters could use the FCC as a mechanism for defining rules under clear statutory guidance. Having an expert agency in place to adjudicate the scope of CALEA's applicability to evolving telecommunications services has been critical to assure that the goals of the statute are satisfied as telecommunications services evolve. The FCC has a vital role both in assuring that carriers meet their obligations so that the Congressional goals of protecting innovation, privacy and security are met in the face of changing technology. In sharp contrast, the vast majority of products and services of concern to law enforcement -- from smartphone hardware devices to operating system software to apps and web-based services -- are largely unregulated by the FCC. Broadly speaking, the Internet and mobile industries, by contrast, do not fall under the purview of any single statute or regulatory agency. So even if Congress were to extend specific law enforcement assistance requirements to Internet platforms and mobile device industries, it is not clear how those requirements could be formulated to assure the proper balance of effectiveness and flexibility.

[20] 47 USC 1001, *et seq*.

Second, the telecommunications industry regulated under CALEA was made up of mature companies provided stable, highly standardized and slow-to-change product offerings. The fact that all of the major telecommunications carriers offered more or less the same kind of services meant that Congress could write one common set of rules for CALEA compliance that would apply in a coherent way to all telecommunication services. CALEA drafters, including this committee, were especially concerned that Congress avoid dictating specific technology so only wrote functional requirements into the statute.[21] However, this created some risk that neither the industry nor law enforcement would know whether a specific technology or service was actually CALEA compliant. To strike the right balance between law enforcement needs for effective access and industry needs for compliance certainty and technical flexibility, Congress created a safe harbor mechanism by which industry could work through its own technical standards bodies to develop technical standards the defined CALEA compliant services.[22] Any company complying with these industry standards is presumed to be in compliance with the statute unless law enforcement specifically challenges the design of those standards. In this way, industry is free to design its own technology and still have certainty that is complying with the law. The fact that there was one main technical standards body that defined the standards for basic telecommunications services was key to statutory architecture of CALEA.

In sharp contrast to the standards-drive development of the telecommunications industry, many of the innovative new services offered by today's Internet platforms, mobile device makers and apps developers are introduced into the market long before they can be standardized. They represent a highly diverse set of companies which varied and highly competitive business models. Product and service offering change rapidly. Of course this is one of reasons way law enforcement faces real challenges in this area. While the Internet and the Web depend on technical standards for global interoperability, those standards are much more generic in nature and do not tend to define full product offerings.

Finally, CALEA was aimed solely at assuring the preservation status quo surveillance capabilities - access to voice communications service that had been functionally unchanged since the original federal wiretap laws were passed in the 1960s. By contrast, the wealth of information available on today's smartphones and other Internet communications and information

[21] 47 USC 1002(a)(1)-(4).
[22] 47 USC 1006(a).

applications is vast and still growing. Everything from exchange of photos, video, personal financial data, real time health monitoring, and location data are available in today's advanced Internet environment. Defining what data should and should not be available to law enforcement will be a complex and ever-changing task. All of these factors give rise to serious doubt as to whether it will be possible to develop and impose a single, top-down regulatory framework to address the wide range of applications and services in which law enforcement could face surveillance challenges.

Even if some regulation existed that maintained security while providing law enforcement access, it is unlikely that the US alone could limit the use and distribution of encryption software. In the years since the years since CALEA was enacted and the Internet marketplace has exploded around the world, the ability for US regulation to control the global availability of encryption software has declined dramatically. A recent study by Harvard's Berkman Center showed that a vast number of products providing cryptographic services originated overseas, including a number of secure messaging and email applications.[23] Any law enacted in the US would therefore only cover a small subset of current encryption apps and have little ability to prevent the development of strong security products abroad. Consider Github, a global social network for collaborative software development, which boasts a userbase of over 14 million developers and 35 million projects.[24] That same site has over 32 million visitors per month, only about a quarter of which are from the US.[25] Once source is shared over such services, it can easily be modified, strengthened, or examined for bugs by programmers from all over the world.

III. Finding a constructive way forward

None of the cautions above in any way diminish the real need that law enforcement has to be able to investigate crimes and gather evidence toward convicting those who break the law. As this committee and the House Judiciary Committee move forward with exploration of this issue

[23] https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html
[24] https://github.com/about/press
[25] http://venturebeat.com/2015/06/17/github-by-the-numbers-32m-people-visit-each-month-74-from-outside-the-u-s-36-from-europe/

through the encryption working group[26] announced last month, addressing the following issues can help identify constructive paths forward.

A. Learn from law enforcement cases

As the pace of law enforcement investigations involving smartphones and other platforms with strong encryption moves forward, there will be much to learn about the nature of the challenges faced by law enforcement, about judicial responses to law enforcement requests for assistance, and about the means chosen to collect information necessary for investigations. Most notably, there will be those cases where enhancing law enforcement technical sophistication can alleviate the need for court orders compelling company assistance. The encryption task force should learn as much as possible about this class of capabilities. Key issues to explore include:

- How can federal law enforcement agencies develop increased online digital investigative prowess? In this regard I strongly endorse the recommendations made by my colleague Susan Landau, Worcester Polytechnic Institute, in her testimony on this issue before the House Judiciary Committee on March 1 of this year. Prof. Landau calls for increased resources to assist the FBI in online digital investigations and forensics.[27]
- In what circumstances will technical assistance from Internet platform, mobile device and apps vendors be needed?
- Of the assistance requests made through the court system or privately between law enforcement and tech companies, what types of requests create risk to the security and privacy of the infrastructure as a whole and what types of assistance can be provided with low security and privacy risk? Answering these questions requires access to detailed information about the nature of these assistance requests, much of which is under seal.
- As the locus of criminal activity moves more to Internet and mobile platforms, to what extent does good access to metadata, including location information, personal health monitoring information, and other Internet-of-Things related sensor data provide alternatives to law enforcement when they are not able to get access to the encrypted content of communications? We know from computer science research that careful automated analysis metadata can be even more revealing than content. New analytic techniques have shown that even without access to the content of communications it is

---

[26] https://judiciary.house.gov/press-release/goodlatte-conyers-upton-pallone-announce-bipartisan-encryption-working-group/

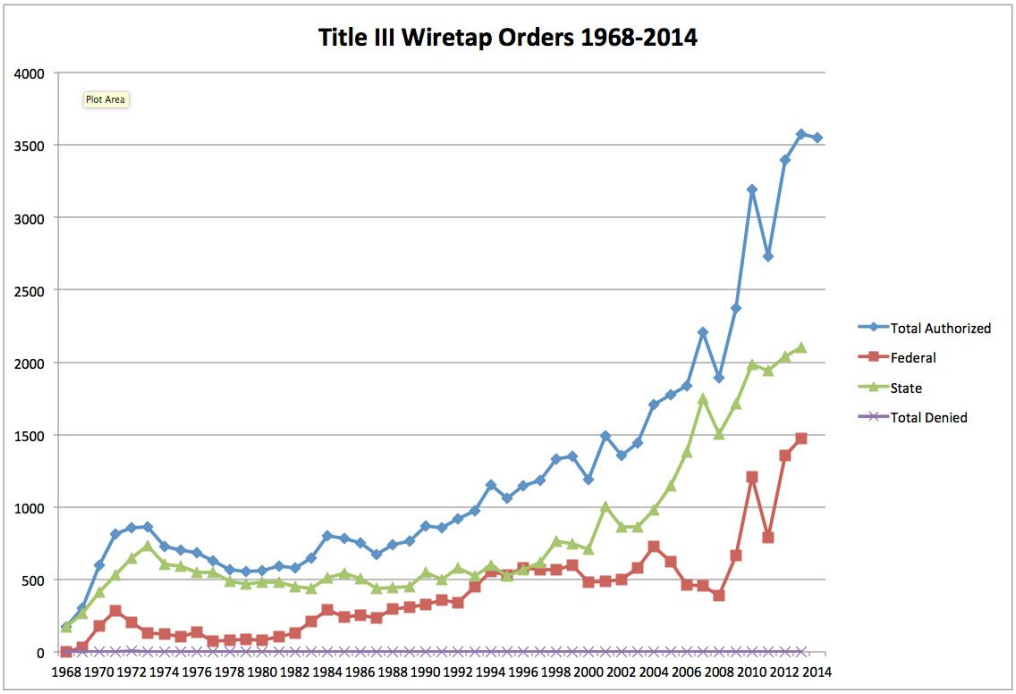
[27] https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf

possible to infer to a very high degree of accuracy a subject's close associates, the identify of intimate partners[28], typical patterns of daily travel,[29] sexual orientation,[30] and other details of private life.

B. Plan for scale

Any long run policy governing the scope of assistance required of tech companies must account for the likely large number of those requests across the country, and the world. As awareness of law enforcement assistance requests moves beyond the request to help with "just one phone," we must consider how an assistance request would look if it were repeated ten, one hundred, or one thousand times.

Figure 1



Source: Administrative Office of the US Courts, Electronic Privacy Information Center

[28] Backstrom, Lars, and Jon Kleinberg. "Romantic partnerships and the dispersion of social ties: a network analysis of relationship status on facebook." *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 2014.
[29] Gonzalez, Marta C., Cesar A. Hidalgo, and Albert-Laszlo Barabasi. "Understanding individual human mobility patterns." *Nature* 453.7196 (2008): 779-782.
[30] Jernigan, Carter, and Behram FT Mistree. "Gaydar: Facebook friendships expose sexual orientation." *First Monday* 14.10 (2009).

The rate of growth of electronic surveillance requests as shown in Figure 1 suggests that the suitability of any policy will be judged in part based on how will scale to large numbers of requests. Consider that most of the individual All Writs Act cases in which the FBI seeks assistance from mobile device manufacturers appear to be one-off requests. However, if those cases gave rise a general rule requiring such assistance, then those companies would have to design systems to respond to large numbers of requests at a time. While a single order to assistance might pose only low security risk, building systems to respond to repeated requests could substantially increase the risk that security sensitive software or private keys might leak out to hostile adversaries. Understanding the nature of these risks requires careful analysis of the nature of the rules derived from these court orders and the design of the systems put in place to enable expeditious response.

C. Rebuild public trust

One of the many lessons to be learned from the last few years of debate about surveillance, privacy and security policy is that the public harbors serious doubts about whether they can trust either industry or government to respect individual privacy. According to the Pew Research Center, 65% of the country believes that there should be stronger limits on government surveillance.[31] And even before the Snowden revelations, more than half of smartphone users uninstalled an app because they were concerned about how information was going to be shared. [32] So a significant portion of the public perceives a real gap in the degree to which the legal system protects them from unwanted privacy intrusion.

Two measures can help close this trust gap and reduce the public anxiety about lawful government surveillance. First, Congress should provide for the maximum feasible transparency regarding legal surveillance orders and operations. As the scope of surveillance grows and given the likely increase in lawful hacking, it is important that the public and policymakers have full visibility into surveillance practices. That visibility is required in order to provide accountability and give policy makers the information necessary to keep surveillance law updated in the face of new technology and changing investigative practices. Second, Congress should continue its efforts to modernize civil liberties and consumer privacy protections in light of advancing technology. The House Judiciary Committee's recent action to provide greater protection for

[31] http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf
[32] http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

private information stored in cloud computing services will offer the public welcome new assurances of basic digital privacy rights. And there are numerous uses of citizens' personal information by the commercial section that deserve stronger legal privacy protections. Personal data collected from mobile devices, personal health monitor, home environmental monitoring and many of sources are being used in a growing variety of innovative new services. We should welcome these new services but also recognize that citizens deserve clear privacy protection in these arenas. By providing clear privacy rules of the road, Congress can ease individual privacy anxiety as to both commercial and government uses of personal data.

D. Strong Security, Privacy and Innovation Guarantees are Vital Complements to Surveillance Law

Finally, however surveillance law and practice evolves, Congress should continue the longstanding tradition of ensconcing privacy and security protections as vital complements of surveillance law. In enacting CALEA, Congress recognized that as surveillance power grows, it is also vital extend privacy and security protections alongside. CALEA explicitly prohibits telecommunications carriers from taking steps to help law enforcement in ways that would impair customer privacy. All CALEA compliant technology is required to be designed so that it has

> "...a minimum of interference with any subscriber's telecommunications service and [is designed] in a manner that protects …. the privacy and security of communications and call-identifying information not authorized to be intercepted."[33]

Congress went even further to guarantee that CALEA surveillance requirements could not be used to block the deployment of any new technology. Under the explicit terms of the statute, if a new technology is being deployed and there is no way for it to meet CALEA requirements, then innovation takes precedence over surveillance guarantees.[34]

---

[33] 47 USC 1002(a)(4)

[34] 47 USC 1002(b)(1)(B). "This subchapter does not authorize any law enforcement agency or officer … to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services." As the legislative history on this section goes on to explain, "The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies…. This means that if a service of technology cannot reasonably be brought into compliance with

None of this is to say that CALEA mandates should be extended to Internet platforms of mobile device manufactures, but rather to recognize that surveillance conducted under law must also respect the privacy of users who are not specific targets of a surveillance order.

Conclusion

While there is not likely to be a 'one size fits all' approach to the challenges that law enforcement faces today and in the future, there are a number of avenues Congress can explore to be sure that legitimate public safety needs are met to the maximum extent possible without compromising the security of Internet users.

* * * * *

the interception requirements, then the service or technology can be deployed." House Report No. 103-827, Part I .