Testimony by Peter Swire
Huang Professor of Law and Ethics
Scheller College of Business
Georgia Institute of Technology

Senate Judiciary Committee Hearing
"Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"
July 8, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to testify today on "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy." I am Peter Swire, the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. I have worked on encryption issues as a government official and scholar for two decades, including recently as a member of President Obama's Review Group on Intelligence and Communications Technology. A more detailed biography is attached to the end of this testimony.

My testimony today is in three parts. First, the Review Group report concluded that strong cybersecurity and strong encryption should be vital national priorities. Our Recommendation 29 stated:

> "We recommend that, regarding encryption, the US Government should:
> (1) fully support and not undermine efforts to create encryption standards;
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
> (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

The Review Group unanimously and clearly recommended that the U.S. Government vigorously encourage the use of strong encryption. With full awareness of the "going dark" concerns, we sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny. Based on the top-secret briefings and our experience, we found these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

Second, it is more accurate to say that we are in a "Golden Age of Surveillance" than for law enforcement to assert that it is "Going Dark." In previous writings,[1] I have agreed that there are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities due to changing encryption technology. These specific losses, however, are more than offset by massive gains, including: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create digital dossiers about individuals' lives.

The testimony specifically shows the enormous gains to law enforcement resulting from adoption in the past twenty years of digital smartphones and text messaging, the two areas most highlighted by law enforcement as examples of "going dark." Although relatively few text messages were sent twenty years ago, by 2010 the number exceeded 6 trillion texts per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs.

For text messages, it might be tempting to say that law enforcement could call the glass half-empty (some texts are encrypted) or half-full (some texts are in the clear). With over six trillion messages filling the cup, though, it takes chutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.

Third, government-mandated vulnerabilities would threaten severe harm to cybersecurity, privacy, human rights, and U.S. technological leadership, while not preventing effective encryption by adversaries.

As occurred in the 1990's, a diverse coalition of cybersecurity experts, technology companies, privacy experts, human rights activists, and others has expressed vociferous and united opposition to government-mandated encryption vulnerabilities.[2] My testimony highlights some of these concerns:

- Technology companies, even before Snowden, had multiple reasons to deploy strong encryption to enhance cybersecurity and customer trust. The ongoing development of encryption should thus not be seen primarily as a short-term response to Snowden's revelations.
- Overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption. A new report issued on July 7 is just the most recent, credible explanation of these technical issues.

---

[1] Peter Swire & Kenesa Ahmad, *'Going Dark' Versus a 'Golden age for Surveillance'*, CENTER FOR DEMOCRACY AND TECHNOLOGY, Nov. 28, 2011 (*available at* https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/).

[2] For one coalition letter, see https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

- U.S. Government support for encryption vulnerabilities increases cybersecurity problems in the "least trusted countries" and globally, and undermines U.S. human rights policies. The United States should be a strong example for cybersecurity and human rights, rather than an excuse used by repressive regimes to surveil U.S.-based businesses and individuals and clamp down on political dissent.
- Mandated vulnerabilities are bad industrial policy – they threaten U.S. technological leadership without preventing bad actors from using strong encryption.

In conclusion, providing access exceptions for U.S. law enforcement and intelligence agencies will be harmful, rather than helpful, to national security. Despite concerns of "going dark," the steady increase of electronic communications worldwide provides these agencies with an ever-growing amount of valuable data and meta-data to use in identifying and pursuing targets of investigations. The inability to directly access the content of a small fraction of these communications does not warrant the subsequent damage that would result to privacy and to U.S. economic, diplomatic, and security interests.

I. Review Group: Strong Cybersecurity and Strong Encryption are Vital to National Security

In August, 2013 President Obama named me as one of five members of the Review Group on Intelligence and Communications Technology, to recommend policies in the wake of the Snowden revelations. Our report emphasized in strong terms the need for strong cybersecurity and strong encryption, without creating vulnerabilities for government access.[3] The Review Group unanimously found these issues essential to achieving national security and other national goals in globalized information networks.

Multiple kinds of evidence support giving credence to the Review Group recommendations. The President's tasking to the group made national security the first priority, along with other considerations such as relations with allies, economic effects, privacy and civil liberties, maintaining public trust, and addressing insider threats. The make-up of the group, along with my own role, showed a commitment to national security, informed by expertise in meeting each of these goals: Richard Clarke has served as cybersecurity coordinator and also anti-terrorist coordinator to Presidents of both political parties; Michael Morell has thirty years of experience in the intelligence community, including serving as acting Director of the CIA; both Cass Sunstein and Geoffrey Stone are eminent legal scholars, with particular

[3] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technology" (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

expertise, respectively, in cost/benefit policy analysis[4] and how to trade off security and civil liberties in times of crisis.[5]

The Review Group, in addition to the expertise of the members, received detailed briefings on encryption, cybersecurity, and related topics at the most highly classified levels. We met personally with top officials in meetings at the NSA, CIA, FBI, and elsewhere. We received particularly detailed briefings on national capabilities in encryption and decryption due to the NSA's leading role on encryption issues and also its Information Assurance Directorate's leading role in cybersecurity defense.[6]

Clear evidence establishes positive recognition of the Review Group's report and recommendations. Along with widespread coverage in the press, the Princeton University Press re-issued the Report in a paperback edition – the first time a federal report has received such treatment since the 9/11 Commission Report. President Obama and his administration have adopted numerous of our 46 recommendations; we have been told that the administration has adopted at least 70% of the recommendations in letter or in spirit. In addition, Congress has found the Report helpful. Each of the major provisions of the USA FREEDOM Act is consistent with one or more of the Review Group's recommendations.[7]

Based on the top-secret briefings and the knowledge of the members, the Review Group unequivocally recommended the following: strong encryption, without backdoors, is essential to cybersecurity, national security, and the prevention of cyber-crime. The Review Group was aware of law enforcement and intelligence agency concerns about "going dark." We simply found no basis for weakening cybersecurity due to the going dark arguments.

Our discussion highlighted the central role of effective encryption for our global communications infrastructure generally, and specifically to address the "massive increase in cyber-crime":

> "Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the

---

[4] Cass Sunstein, along with his numerous publications, served as Administrator for five years for the Office of Information and Regulatory Affairs of the U.S. Office of Management and Budget, which oversees cost/benefit analyses of federal regulations. http://hls.harvard.edu/faculty/directory/10871/Sunstein.

[5] Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from The Sedition Act of 1798 to The War on Terrorism* (2004), *Top Secret: When Our Government Keeps Us in the Dark* (2007), *War and Liberty: An American Dilemma* (2007).

[6] See https://www.nsa.gov/ia for information on the IAD's role and activities.

[7] Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years*, IAPP PRIVACY PERSPECTIVES, Jun. 8, 2015 (*available at* https://privacyassociation.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years).

entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.

"The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world. Encryption allows users of information technology systems to trust that their data, including their financial transactions, will not be altered or stolen. Encryption-related software, including pervasive examples such as Secure Sockets Layer (SSL) and Public Key Infrastructure (PKI), is essential to online commerce and user authentication. It is part of the underpinning of current communications networks. Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud."

Based on this analysis of the problem, we recommended vigorous U.S. government support for effective encryption, including a ban on subverting the security of generally available commercial products and services:

"Recommendation 29: We recommend that, regarding encryption, the US Government should:
(1) fully support and not undermine efforts to create encryption standards;
(2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
(3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

Our concern with cyber-crime and cybersecurity extended to our discussion of cyber-vulnerabilities, including "Zero Day" attacks, defined as attacks where developers have had zero days to address the vulnerability. Review Group Recommendation 30 emphasized that vulnerabilities should be "quickly blocked, so that the underlying vulnerabilities are patched on US Government or other networks." The Review Group recommended that, "when an urgent and significant national security policy can be addressed" by leaving a vulnerability unpatched, an agency of the US Government may be authorized to use the vulnerability "temporarily," instead of "immediately fixing the underlying vulnerability." Allowing the vulnerability to remain unpatched should be subject to "a senior-level, interagency approval process," chaired by the National Security Council. To ensure that multiple perspectives are included before allowing such vulnerabilities, we

wrote that the process should involve "all offices and departments with relevant concerns, generally including the National Economic Council, State, Commerce, Energy, and Homeland Security."

In conclusion on the Review Group, we unanimously and clearly recommended that the U.S. Government vigorously encourage the use of strong encryption. With full awareness of the "going dark" concerns, we sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny. Based on the top-secret briefings and our experience, we found these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

II. Going Dark vs. a Golden Age of Surveillance

In 2011, I co-authored an article that has been widely cited in the encryption debates: "Going Dark vs. a Golden Age for Surveillance."[8] We did not agree that the FBI and other agencies are "going dark." We acknowledged that, "due to changing technology, there are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities." We continued: "These specific losses, however, are more than offset by massive gains. Public debates should recognize that we are truly in a golden age of surveillance. By understanding that, we can reject calls for bad encryption policy." The four years since writing that article, including my experience in the Review Group, have reinforced my confidence in these conclusions. The "going dark" claim is fundamentally incorrect; instead, government agencies are operating in a "golden age of surveillance."

In this part of the testimony, I critically examine law enforcement statements about how common the "going dark" problem is. I then explain the basis for concluding that we are instead in a "golden age of surveillance," and apply the analysis to encrypted text messaging and encrypted smartphones.

A. Challenges facing law enforcement access. FBI Director Comey's article this week in LawFare highlights law enforcement concerns about "going dark." Notably, Director Comey says that "our conversations and our 'papers and effects' will be locked in such a way that permits access only by participants to a conversation or the owner of the device holding the data."[9] Although I agree that there are certain subsets of communications that may not be reachable with a court order, Director Comey's statement is so over-broad that policymakers should be

---

[8] Peter Swire & Kenesa Ahmad, *'Going Dark' Versus a 'Golden age for Surveillance'*, CENTER FOR DEMOCRACY AND TECHNOLOGY, Nov. 28, 2011 (*available at* https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/).

[9] James Comey, "Encryption, Public Safety, and "Going Dark," July 6, 2015, http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

extremely cautious about drawing policy conclusions from the assertion. Notably, Director Comey's statement essentially ignores the pervasive fact of cloud backup of content, and also greatly over-states the extent to which emails or other relevant content is or will be "dark" to law enforcement.

Before looking at the factual details, I pause to emphasize my support for highly effective law enforcement and intelligence activities to promote public safety and national security. My previous government work and other experience have given me considerable sympathy and, I believe, insight about the challenges facing law enforcement and intelligence agencies. During my time on the Review Group, for instance, one of my sons was serving as platoon leader for a motorized infantry unit in Kandahar. I can assure you that I wanted our signals intelligence to be absolutely outstanding to prevent an IED or other remote-control threat from harming his patrol. In 2000, the President's Chief of Staff entrusted me to serve as Chair of a White House Working Group on how to update wiretap laws for the Internet. That process included all of the major law enforcement and intelligence agencies, and resulted in a cleared administration bill, accepted by those agencies, that was later introduced in the Senate by Senator Leahy. Along with these years of experience working on law enforcement issues, I note that as a law student I worked for the Manhattan District Attorney's office, represented today by its leader, Mr. Vance. Doing a police ride-along for a night in Harlem is one of many experiences that has given me a vivid appreciation for how our police officers put themselves in harm's way as they face criminals and other threats to our public safety.

I have written previously about the central importance of cloud back-up and other stored records as a feature of law enforcement access to communications.[10] There are numerous reasons why content on a modern smartphone or computer is very typically stored on the cloud, including the need for back-up and the ability for individuals or enterprises to access important information from different devices. In addition, the standard operation of a huge portion of apps on a smartphone includes automatic reporting of information to the app developer or others. For information scored in such cloud settings, standard functionality by the cloud provider means for a very wide range of applications that information is viewable by the cloud provider and not encrypted for access only by the user.

Despite concerns from law enforcement about end-to-end encryption (where content can be viewed only by the sender and recipient), my view is that the government in the vast majority of cases has retained and will retain access to plaintext of the content. For corporate accounts, the government can readily submit a court order to the corporate IT department, which will then turn over the content on pain of contempt of court. For individual email accounts, the government remains in a similarly strong position. The portion of individuals who use who end-to-end encryption remains vanishingly small. All of the largest email providers

[10] "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," International Data Privacy Law (2012), doi: 10.1093/idpl/ips025.

today retain the ability to access the plaintext of emails when served a court order. Individuals who use smaller providers can choose end-to-end encryption (where the contents are available only to the sender and recipient), but few do so due to the high risk of problems – users who lose their keys lose access to all of their emails. How many of us would manage access to our bank accounts or other important accounts without the possibility of assistance if we forget the password? The risk of losing all access to one's communications is an enormous barrier to adoption. That is the single biggest reason in my view that I continue to doubt that we will see widespread adoption of end-to-end encryption.

In short, law enforcement may face small subsets of circumstances that match Director Comey's stated concern: locked devices or end-to-end encryption ("access only by the participants to a conversation"). At a factual level, however, we should remain highly alert to over-broad assertions about the pervasiveness of such "going dark."

B. Greater recent gains for lawful access.

The discussion here highlights three areas where law enforcement has far greater capabilities than ever before: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create "digital dossiers" about individuals' lives. This information about any individual suspect is made even more useful because of the way that Big Data and data mining can help identify suspects.

1. Location information. Knowing the location over time of a suspect or witness is an enormous boon to law enforcement. For the first time in human history, we live in an age where most people carry a tracking device, the mobile phone. Location information comes standard with a wireless network – the phone company needs to know where your phone is to send you the call. A specific cell handles the call, so the network knows what cell you are in. Location information is tremendously useful for law enforcement and national security agencies. It can put a suspect at the scene of a crime, or establish an alibi. It can act as a "bug" without the need for the agency to place a bug on the suspect's person or property.

Even for the few who don't carry a phone, location is getting far more difficult to hide. Video surveillance cameras exist in stores, gas stations, and a proliferating variety of other places. Our cars' locations are tracked by EZ Pass, parking garages, and many more. Going forward, as the Internet of Things multiplies the sensors in daily life, we will see an exponential increase in the density of records about our individual location. When it comes to location, the maps are increasingly lit up for law enforcement, and emphatically not dark.

2. Meta-data reveals confederates and co-conspirators. The debates since Snowden have sensitized us all to the power and importance of meta-data. Congress, in the USA-FREEDOM Act, recently set important new limits on

government bulk collection of meta-data, precisely out of recognition of how much meta-data reveals.

The explosive increase in meta-data provides unprecedented information to law enforcement and intelligence agencies about a suspect or witness' confederates and co-conspirators. For many investigations, *who* is called is at least as important as *what* is said in the call. The investigator gets leads on whom else to investigate and can follow those leads to the contact's contacts, and so on. Nothing in the USA-FREEDOM Act limited the ongoing expansion of meta-data held by the private sector.

The importance of confederates has become famous in social networking. The term "social graph" was coined in connection with social networks to describe the phenomenon of "the global mapping of everybody and how they're related."[11] For investigatory agencies, mapping everybody and how they are related is extremely useful.

At some level, all of us realize the rapid increase in the density of our communications in recent years. The Pew Foundation, for instance, reports that 8% of Internet users were on social media in 2005, compared with 61% in 2010 and 74% in 2014.[12] With wireless phones and unlimited calling plans, the volume of our phone calls has skyrocketed, documenting in detail whom we speak with. VoiP calls through services such as Skype and Facetime similarly document the to/from information. E-mails have become a pervasive feature of life for many people; the emergence of global web mail providers, and nationwide service of process provided in the USA PATRIOT Act, gives agencies the convenience of serving many lawful requests to a small number of providers. Techniques for masking meta-data enormously lag behind current encryption techniques for content.

Our wireline, wireless, and VoiP calls, along with texts and social networking records are treasure troves of information for investigatory agencies. In the bygone era of face-to-face communications, no trace was usually left regarding whom a suspect had talked with. Today, by contrast, an individual would need to abstain from many everyday activities, over a period of years, to prevent the government from obtaining information about his or her contacts. The identity of those contacts helps lead investigators to additional targets of interest, thereby painting a broader and more precise picture of potential criminal or national security activity.

3. Digital dossiers and Big Data. Information about location and a person's confederates, in turn, are simply examples of the larger trend towards detailed personal records. Privacy scholars and regulators such as the Federal Trade Commission have documented the multi-dimensional expansion of personal

[11] http://www.cbsnews.com/stories/2010/04/21/tech/main6418458.shtml.

[12] http://www.pewinternet.org/data-trend/social-media/social-media-use-all-users/

information in the hands of data brokers,[13] banks, hospitals, online advertisers, government agencies, and other record holders.[14] The new era of "Big Data" includes advanced analytics that are to mine the data in these numerous databases. Although a few people attempt to live "off the grid," this is not a feasible option for the vast majority of citizens in developed countries. Once an individual is identified as a target, the government – via lawful process – can access information specific to that individual in unprecedented detail.

C. Going Dark vs. Golden Age for text messages. Two areas of concern that law enforcement has highlighted have been the possibility of end-to-end encryption for text messages and new policies for mobile devices that ensure there is no "master key" to allow law enforcement access to the device. For both of these examples, the law enforcement claims to "going dark" turn out, upon inspection, to validate the view that we are in a golden age of surveillance.

For text messages, law enforcement has expressed concerns that some software, such as iMessage and WhatsApp, provides end-to-end encryption of the content. The idea of "going dark" is that law enforcement has lost something – they used to be able to see something, and now it is dark. But that is not what has happened. Not so long ago, there were no text messages – in almost all instances, daily communications never created a record of content, because we spoke to someone in our presence, or called someone on a non-wiretapped phone.

A much more accurate comparison with past practice is that law enforcement has gained an inestimable boon – the recorded meta-data of text messages. The history of SMS (short message service) illustrates the point. According to one source, the number of SMS sent by a typical cell phone user in 1995 was .4 per month, rising to 35 per user per month by 2000. By 2010, when per-text charges for text messaging were becoming obsolete, an estimated *6.1 trillion* SMS text messages were sent, in addition to the enormous quantity of text messages sent through Facebook Messenger, WhatsApp, and other data text services.[15]

For text messaging, therefore, law enforcement has experienced the new brightness of literally trillions of text messages per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs.

---

[13] FED. TRADE COMM'N, DATA BROKERS A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) (*available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

[14] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (*available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313301).

[15] The statistics here are taken from https://en.wikipedia.org/wiki/Short_Message_Service; ITU, THE WORLD IN 2010 ICT FACTS AND FIGURES (2010) (*available at* http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf).

For text messages, it might be tempting to say that one can call the glass half-empty or half-full for law enforcement. With over six trillion messages filling the cup, though, it takes chutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.

D. Going Dark vs. Golden Age for device encryption. Historical perspective similarly helps us understand going dark vs. a golden age of surveillance for smartphones. Two decades ago, a typical arrest rarely resulted in police access to a cell phone – mobile phones were fairly rare. A decade ago, a typical arrest might turn up a flip phone, with small amounts of meta-data about who had sent and received recent calls. Today, many users carry smart-phones with gigabytes of data, an almost unimaginable cornucopia of investigative detail in texts, emails, photos, and other apps. It is essentially impossible to describe this historical trajectory as the police "going dark." Before, they had little or nothing. Today, they often have a cornucopia.

The law enforcement response is basically that they don't always get the cornucopia, or sometimes they only get most of the cornucopia. Let's begin with the basics, whether law enforcement gets any access to what is in the device. First, many users today don't even put a passcode on their phone – anyone who picks it up can access the information. Second, if a suspect does use a passcode, many users have no encryption of data on the phone or there are technical ways to evade the encryption implementation. Third, especially in our world where confederates and co-conspirators are so easy to identify, the prosecutors only have to grant immunity to one co-conspirator in order to gain entry into the content shared with the other suspects. Fourth, the courts have yet to resolve how the Fifth Amendment privilege against self-incrimination applies to opening an encrypted smartphone, especially in a "going dark" scenario; the courts may decide that the government can jail suspects for contempt if they refuse to open the phone. Biometric identification, which is increasingly used for smartphones, may be especially available to law enforcement without triggering the privilege. These four reasons may help explain why it has been so difficult for the FBI and other law enforcement officials to provide examples of where encryption has frustrated an investigation, and the most recent statistics actually show a decline in wiretaps encountering encryption in 2014 compared to 2013, hardly evidence of "going dark."[16]

Even where law enforcement does not gain access to the device (the cornucopia), law enforcement can often get most or all of the relevant data (most of the cornucopia). I have already discussed much of the data that remains available to

[16] According to the federal 2014 Wiretap Report: "The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. In two of these wiretaps, officials were unable to decipher the plain text of the messages. Three federal wiretaps were reported as being encrypted in 2014, of which two could not be decrypted. Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. Officials were able to decipher the plain text of the communications in four of the five intercepts." http://www.uscourts.gov/statistics-reports/wiretap-report-2014

law enforcement without recourse to the device itself – location of the phone; plaintext of emails; meta-data and often plaintext for text messages; and social networking data showing confederates. In addition, as discussed above, cloud storage often exists for numerous other data-sets, such as cloud storage of photos and videos, location on apps such as Waze and Uber, banking and other financial apps showing purchases, and so on. Indeed the increasing norm is full-device backups to the cloud. Even for an inaccessible device, therefore, the full content may be available from an accessible cloud provider.

E. Summary on Going Dark vs. Golden Age. To summarize, law enforcement does confront important challenges as encryption and other effective cybersecurity mechanisms become more pervasive. There will be particular instances where a lawful court order will not generate the full text of a communication. Nonetheless, numerous other technical trends are moving sharply in the direction of unprecedented law enforcement access. If the agencies had the choice between 1990-era capabilities or capabilities today, they would choose the capabilities today.

III. Government-Mandated Vulnerabilities Would Threaten U.S. Technological Leadership, While Not Preventing Effective Encryption by Adversaries

While national security interests are, justifiably, the focus of the current discussion around encryption, any mandated vulnerabilities would have far reaching effects in other sectors of U.S. interest as well. The first "Crypto Wars" in the 1990's are illustrative of the futility of this approach: attempts to control the export of encryption negatively impacted U.S. business interests while other players entered to provide their own encryption solutions. Any mandated weakening of U.S. encryption today would create similar issues, as consumers both at home and abroad demand strong, independent encryption for a variety of reasons. Hamstringing U.S. companies from being able to meet this demand will only benefit foreign competitors who seek to fill the void while giving political cover for those countries who will demand similar access in order to further the suppression of targeted speech and oppression.

A. Technology companies, even before Snowden, had multiple reasons to use strong encryption to enhance cybersecurity and customer trust.

Although encryption issues have become the subject of greater public debate since the beginning of the Snowden revelations, there has been an ongoing trend to deploy effective encryption for consumer and business applications. The central importance of encryption to cybersecurity was a major theme in the Review Group report, as discussed above. Strong encryption is essentially the broadest-spectrum antibiotic against cyber-infections. In our era of pervasive cyber-attacks, encryption is crucial to preventing identity theft, reducing the harmful effects of data breaches, and providing myriad other protections against attacks.

The necessary and pervasive spread of encryption was the topic of my 2012 article why encryption drives the government to seek access to the cloud, cited above. That article gave a 2012 list of examples of widespread encryption:

- "Corporate and government users have widely adopted Virtual Private Networks (VPNs) for remote users. VPNs are strongly encrypted, thus protecting the organization's emails and other communications.
- Electronic commerce, including credit card numbers, is overwhelmingly conducted today using SSL (Secure Sockets Layer).
- Facebook now supports SSL. If it enables SSL by default [which is true in 2015], then its social networking communications would not be readable at the ISP level.
- Research in Motion's Blackberry products use strong encryption, and RIM itself does not have the keys for corporations who manage keys themselves.
- Major web locker services, such as Dropbox, use SSL by default.
- Skype, the leading VoIP provider, encrypts end-to-end. Many international calls are made using Skype. VoIP enables voice communications to be encrypted at scale.
- Many Internet games and other services use encryption, often with accompanying voice and chat channels."[17]

This trend has continued since 2012, including for the device encryption of smartphones that the FBI has criticized.[18] Although it might seem that the widespread use of encryption is a reason to mandate vulnerabilities in software to enable law enforcement access, my view is different. The growing and pervasive use of encryption is recognition of its centrality to defending against cyber-attacks – the ongoing debates about cybersecurity legislation in Congress show a consensus that customers need this protection, and companies need to supply it. In addition, CALEA II-style mandates run up against the pervasive use of encryption. Such

---

[17] "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," International Data Privacy Law (2012), doi: 10.1093/idpl/ips025.

[18] Joe Miller, *Google and Apple to introduce default encryption*, BBC NEWS, Sep. 19, 2104 (*available at* http://www.bbc.com/news/technology-29276955), Klint Finley, *Encrypted Web Traffic More Than Doubles After NSA Revelations*, WIRED, May 16, 2014 (*available at* http://www.wired.com/2014/05/sandvine-report/), Peter Eckersley, *Launching in 2015: A Certificate Authority to Encrypt the Entire Web*, EFF, Nov. 18, 2014 (*available at* https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web), James Vincent, *Microsoft will encrypt Bing search traffic by default*, THE VERGE, Jun 16, 2015 (*available at* https://www.theverge.com/2015/6/16/8788373/encrypted-search-microsoft-bing), Kate Vinton, *Wikipedia Is Now Using HTTPS By Default To Prevent Snooping and Censorship*, FORBES, Jun. 12, 2015 (*available at* http://www.forbes.com/sites/katevinton/2015/06/12/wikipedia-is-now-using-https-by-default-to-prevent-snooping-and-censorship/), Alex Hern, *Facebook introduces PGP encryption for sensitive emails*, THE GUARDIAN, Jun. 1, 2015 (*available at* http://www.theguardian.com/technology/2015/jun/01/facebook-introduces-pgp-encryption-for-sensitive-emails), Micah Lee, *Microsoft Gives Details About Its Controversial Disk Encryption*, The Intercept, Jun. 4, 2015 (*available at* https://firstlook.org/theintercept/2015/06/04/microsoft-disk-encryption/).

mandates would be a regulatory nightmare, affecting so many applications and implementations as to be unmanageable and enormously costly.

B. Overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption.

The technological hopes of law enforcement were expressed in House testimony this April by Amy Hess, Executive Assistant Director of the Science and Technology Branch of the FBI. She said:

> "To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data. We have been on the front lines of the fight against cyber crime and economic espionage and we recognize that absolute security does not exist in either the physical or digital world. *Any lawful intercept or access solution should not lower the overall security."* (emphasis supplied)[19]

The heart of the problem is this: the Review Group and the vast majority of technical experts do not think the FBI's hopes are possible to achieve, for the sorts of access suggested in CALEA II proposals. Even if they assist law enforcement in some respects, the proposed lawful intercept and access solutions lower overall security.

Repeated blue-ribbon panels of technical experts have come to the same conclusion. In the 1990's, Representative Bob Goodlatte summed up the lessons that Congress was learning:

> "Strong encryption *prevents* crime. Just as dead-bolt locks and alarm systems help people protect their homes against intruders, thereby assisting law enforcement in preventing crime, strong encryption allows people to protect their digital communications and computer systems against criminal hackers and computer thieves. The blue-ribbon National Research Council said it best, concluding that strong encryption supports both law enforcement efforts and our national security, while protecting the proprietary information of U.S. businesses."[20]

---

[19] Amy Hess, *Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology*, Apr. 29, 2015 (*available at* https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices).

[20] Bob Goodlatte, "Let's Open Up Encryption," *The Washington Post*, June 12, 1997, *available at* http://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/ocr061297.htm (emphasis added), citing Kenneth W. Dam and Herbert S. Lin, Editors, Committee to Study National Cryptography Policy, National Research Council, "Cryptography's Role in Securing the Information

An influential group of encryption experts issued a 1997 report on "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption."[21] Among the key findings of this technical group: "The deployment of key-recovery-based encryption infrastructures to meet stated specifications will result in substantial sacrifices in security and greatly increased costs to end users." The report made numerous, telling criticisms of key recovery approaches. From my participation in the policy debates of the era, there was no effective technical response by supporters of government key recovery approaches.

In May, 2013, just prior to the first Snowden revelations, the Center for Democracy and Technology gathered a different group of technical experts to write "CALEA II: Risks of Wiretap Modifications to Endpoints."[22] The conclusions about the harms of mandated vulnerabilities were clear:

> "The U.S. government is proposing to expand wiretap design laws broadly to Internet services, including voice over Internet protocol (VoIP) services and other peer- to-peer tools that allow communications in real-time directly between individuals. This report explains how mandating wiretap capabilities in endpoints poses serious security risks. Requiring software vendors to build intercept functionality into their products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security of the United States."

An impressive new technical study by a group of experts was released on July 7, just before this hearing, entitled "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications."[23] It states:

> "We have found that the damage that could be caused by law enforcement exceptional requirements would be even greater today than it would have been twenty years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse "forward secrecy" design

---

Society," *National Academies Press* (1996), *available at* http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society.

[21] Hal Abelson, Ross N. Anderson, Steven Michael Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and others. https://www.schneier.com/paper-key-escrow.html.

[22] https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

[23] "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication." Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Neumann, Peter G.; Landau, Susan; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael; Weitzner, Daniel J.

> practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally-connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws."

The new study highlights three general problems. First, providing mandated access "would force a U-turn from the best practices now being deployed to make the Internet more secure." For instance, best practices now incorporate "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." If law enforcement requires key retention, then that directly undermines the protection against later attacks.

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. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services… 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 for bad actors to target:

> "Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys have guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management 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 because OPM had insecure infrastructure. If service providers implement exceptional

> access requirements incorrectly, the security of all of their users will be at risk."

At a practical level, there are thousands of police departments spread across the United States. Providing online access to these police departments, while having iron-clad assurances that no hackers can get in, ignores the lessons of the recent OPM breach and the numerous other data breaches in the public and private sectors.

Let me add my personal observations on these studies about the technical obstacles to safe key recovery by law enforcement. I have engaged with a wide range of technical encryption experts for two decades, both inside and outside of government, often as the only person with legal training at a conference. I have an appointment in the College of Computing at Georgia Tech, and teach cybersecurity there, with a majority of the class in graduate studies in information security. Based on this engagement with technical experts, they say the same things in private as are written in the blue-ribbon reports. The passion that the most eminent technical experts show here is due to their conviction based on hard-fought experience, and not as a lobbying ploy.

Quite simply, the technical experts I trust believe that the FBI is asking for the impossible. CALEA II-style proposals hurt security.

C. U.S. Government support for encryption vulnerabilities increases cybersecurity problems in the "least trusted countries" and globally, and undermines U.S. human rights policies.

U.S. Government support for encryption vulnerabilities not only encounters the severe technical cybersecurity problems just discussed, but also increases the likelihood of cybersecurity threats originating from other countries. U.S. government support for such vulnerabilities harms both cybersecurity and human rights.

In 2012 I was the lead author of a 65-page law review article on "Encryption and Globalization," a comprehensive examination of global effects of national encryption policies.[24] What we called the "least trusted country" problem is critical to understanding cybersecurity and encryption in our globalized setting. If one country sets limits on encryption, then cross-border communications that comply with that country's laws will have that vulnerability. If one party to a communication uses compromised encryption as required in that country, then those globally who communicate with that country will have their communications compromised as well.

Key escrow provides a vivid example of the least trusted country problem.

[24] Peter Swire & Kenesa Ahmad, "Encryption and Globalization," 13 *Colum. Sci. & Tech. L. Rev.* 416 (2012).

Consider whatever country in the world you trust the least. For India, that could be Pakistan, for Taiwan it could be China, for Israel it could be Iran. (I prefer not to pick one such country for the United States.) How secure would any of these countries be if their least trusted country had key escrow for their communications? We wrote: "Ultimately, laws that limit effective encryption create security holes. Communications that originate, end, travel through, or comply with the policies of those nations are systematically weakened —they are as secure as they would be in the hands of our least trusted country, whatever country that may be… Think about important communications in the hands of the country you trust least in the world. That is the Internet that would result from limits on strong encryption."

In this globalized setting, the United States has a crucial leadership role to play concerning possible compromises in global communications security. I saw this personally when I met in India with senior officials in 2011, when India was considering a sweeping key escrow proposal. In these discussions, we explained the history of the crypto wars in the 1990's, and gave the technical and political reasons why the U.S. government had correctly decided to abandon a key escrow approach. After these discussions, and those with other American and global experts, the Indian government substantially cut back its legal proposal, and also has had far less than full implementation of the residual provisions. In short, the American example was useful in reducing the bad effects on global security, notably including for U.S. individuals and companies communicating abroad. If American policy becomes to mandate encryption vulnerabilities, either in law and practice, then our moral and policy authority to argue for strong cybersecurity is eroded.

The human rights implications of mandating vulnerabilities are also substantial and important. The Review Group Report discussed the importance of the U.S. Internet Freedom agenda, to bolster protections for journalist, religious minorities, and political dissenters around the world, especially in repressive regimes. In February, the U.S. government wrote a detailed statement about the importance of encryption to global free expression and human rights to David Kaye, Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression for the United Nations High Commissioner for Human Rights. Key statements included:

> "As President Obama recently made clear, the United States firmly supports the development of robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote freedoms of expression and association, and strengthen cybersecurity. Encryption, as well as tools that assist with anonymity, are especially important in sensitive contexts where attribution could have negative political, social or personal consequences or when the privacy interests in the information are strong…. Consistent with this legal framework, as a matter of policy, the United States has long supported the development and use of

strong encryption and anonymity-enabling tools online."[25]

The importance of these anonymity-enabling tools has been underscored by financial support, especially from the U.S. State Department, for development of software and platforms to enable human rights activists and others abroad to communicate effectively notwithstanding local political regimes' efforts to undermine such communications. The U.S. government support for its Internet Freedom agenda is broadly consistent with the June 17, 2015 Joint Civil Society Statement by 25 leading non-government organizations entitled "Promote Strong Encryption and Anonymity in the Digital Age."[26]

In conclusion on the "least trusted country" discussion, it is abundantly clear in our globalized world that decisions about U.S. law enforcement access to communications have important effects on how other countries decide to respond to similar issues in their own countries. The Information Technology Industry Council and Software & Information Industry Association made this point in a recent letter: "In addition to these security and trust concerns, the U.S. policy position on encryption will send a signal to the rest of the world. Should the U.S. government require companies to weaken encryption technology, such requirements will legitimize similar efforts by foreign governments. This would threaten the global marketplace as well as deprive individuals of certain liberties. "[27] The United States should be a strong example for cybersecurity and human rights, rather than an excuse used by repressive regimes to surveil U.S.-based businesses and individuals and clamp down on political dissent.

D. Mandated vulnerabilities are bad industrial policy – they threaten U.S. technological leadership without preventing bad actors from using strong encryption.

I next turn to why mandated vulnerabilities are bad as a matter of economic and industrial policy. Such vulnerabilities threaten U.S. technological leadership because they provide a ready excuse for foreign governments and purchasers to eschew American products and services. As we learned from the crypto battles of the 1990's, they also are futile – they encourage non-U.S. suppliers to gain the technical edge in supplying effective encryption.

In April, 2015 House testimony, Kevin Bankston of the New America Foundation summarized key economic arguments:

> "American technology companies, which currently dominate the global market, have already been wrestling with diminished consumer trust in the wake of revelations about the scope of the

[25]http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf
[26] https://www.hrw.org/news/2015/06/17/promote-strong-encryption-and-anonymity-digital-age-0
[27] http://www.itic.org/dotAsset/58fbf8de-cd86-47a0-a114-43a55776d2e6.pdf.

> National Security Agency's programs, a loss of trust already predicted to cost our economy billions of dollars. Any new requirement that those companies guarantee that the U.S. government have the technical capability to decrypt their users' data would give foreign users— including major institutional clients such as foreign corporations and governments that especially rely on the security of those products and services—even more incentive to avoid American products and turn to foreign competitors. It would also likely diminish trust in the security of digital technology and the Internet overall, which would slow future growth of the Internet and Internet-enabled commerce and threaten the primary economic engine of the 21st century. To put it bluntly, foreign customers will not want to buy or use online services, hardware products, software products or any other information systems that have been explicitly designed to facilitate backdoor access for the FBI or the NSA."[28]

The experience from the 1990's shows that foreign suppliers are eager to step into gaps left by U.S. restrictions on encryption. Under the export control regime then in existence, it was illegal to export strong encryption from the U.S. Other encryption suppliers, such as from Russia and Israel, became significant players precisely because U.S.-based companies could not supply effective software encryption from the U.S. In my experience, the futility of the encryption limits was an especially persuasive argument to members of Congress – why should we support an approach that undermined the U.S. tech sector and also didn't stop the spread of strong encryption? A related phenomenon, less well known, was the concern within the Pentagon about the rising competition from non-U.S. technology companies. For the Department of Defense, limits on U.S. encryption development meant that it faced the risk of relying on second-rate encryption for its own systems, while other countries could be developing state-of-the-art encryption that would benefit other militaries but not the United States.

Mandated vulnerabilities within the United States, to assist law enforcement, thus repeat the 1990's syndrome of harm to U.S. industry as well as futility. Much of the growth in encryption-related software and products could come from non-U.S. companies that serve the global market for secure communications and storage. Other growth would come from the already-flourishing free and open source sector. As Bankston wrote:

> "A government mandate prohibiting U.S. companies from offering products or services with unbreakable encryption is of little use when foreign companies can and will offer more secure products and services, and when an independent coder anywhere on the planet has the resources to create and distribute free tools for encrypting your

[28] http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf.

communications or the data stored on your mobile devices. As former Homeland Security Secretary Michael Chertoff recently put it, '[T]hat genie is not going back in the bottle.'"[29]

Stanford cybersecurity research Jonathan Mayer sums up the futility of technology controls justified by "going dark" concerns:

> "Cryptographic backdoors are, however, not a solution. Beyond the myriad other objections, they pose too much of a cost-benefit asymmetry. In order to make secure apps just *slightly* more difficult for criminals to obtain, and just *slightly* less worthwhile for developers, the government would have to go to *extraordinary* lengths. In an arms race between cryptographic backdoors and secure apps, the United States would inevitably lose."[30]

Conclusion

Much more could be added about why such a diverse coalition of cybersecurity experts, technology companies, privacy experts, human rights activists, and others are so passionately concerned about the "going dark" arguments made by law enforcement agencies.[31] We can respect the heartfelt concerns of law enforcement officials facing new challenges while respectfully disagreeing with proposed policies. The policy debates in the 1990s ended in a clear verdict, accepted by Congress and the administration -- effective encryption is essential to our modern communications infrastructure, and mandated weaknesses in encryption are both futile and ultimately counter-productive.

Biography of Peter Swire

Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. He has appointments by courtesy with the College of Computing and School of Public Policy. His courses include "Information Security Strategies and Policy" and "Privacy, Technology, Policy, and Law."

In 2015, the International Association of Privacy Professionals, among its over 20,000 members, awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Prior to that, he was co-chair of the global Do Not

---

[29] Bankston, at http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf, quoting Jason Koebler, "The Man Who Crafted the Patriot Act Now Supports Your Right to Encrypt Data," *Motherboard*, February 27, 2015, *available at* http://motherboard.vice.com/read/the-man-who-crafted-the-patriot-act-now- supports-your-right-to-encrypt-data.

[30] Jonathan Mayer, "You Can't Backdoor a Platform," Apr. 28, 2015, http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform.

[31] For one coalition letter, see https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

Track process for the World Wide Web Consortium.

Swire is Senior Counsel with Alston & Bird, LLP. He is Senior Fellow with the Future of Privacy Forum, a Policy Fellow with the Center for Democracy and Technology, and a Cybersecurity Fellow with the New America Foundation.

Under President Clinton, Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy. In that role, he chaired the White House Working Group on Encryption, and participated in the 1999 White House announcement enabling export of strong encryption. As Chief Counselor, his activities included being White House coordinator for the HIPAA medical privacy rule, chairing a White House task force on how to update wiretap laws for the Internet age, and helping negotiate the U.S.-E.U. Safe Harbor agreement for trans-border data flows. Under President Obama, he served as Special Assistant to the President for Economic Policy.

Swire's writings on encryption include: (1) "The Uses and Limits of Financial Cryptography: A Law Professor's Perspective," chapter in the *proceedings of Financial Cryptography* '97 (Springer-Verlag, 1997); (2) "'Going Dark' vs. 'A Golden Age for Surveillance,'" *Center for Democracy and Technology*, Nov. 28, 2011 (with Kenesa Ahmad); (3) "Encryption and Globalization," 13 *Colum. Sci. & Tech. L. Rev.* 416 (2012) (with Kenesa Ahmad); (4) "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," International Data Privacy Law (2012), doi: 10.1093/idpl/ips025; (5) "Going Dark vs. Going Secure – New CDT Experts Report on CALEA II," *IAPP Privacy Perspectives*, May 16, 2013; (6) "The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance," *Just Security*, Nov. 17, 2014.

Swire graduated from Princeton University, summa cum laude, and the Yale Law School, where he was an editor of the Yale Law Journal.