DON'T PANIC.

Making Progress on the "Going Dark" Debate

Berkman
The Berkman Center for Internet & Society
at Harvard University

Foreword

Just over a year ago, with support from the William and Flora Hewlett Foundation, the Berkman Center for Internet & Society at Harvard University convened a diverse group of security and policy experts from academia, civil society, and the U.S. intelligence community to begin to work through some of the particularly vexing and enduring problems of surveillance and cybersecurity.

The group came together understanding that there has been no shortage of debate. Our goals were to foster a straightforward, non-talking-point exchange among people who do not normally have a chance to engage with each other, and then to contribute in meaningful and concrete ways to the discourse on these issues.

A public debate unfolded alongside our meetings: the claims and questions around the government finding a landscape that is "going dark" due to new forms of encryption introduced into mainstream consumer products and services by the companies who offer them. We have sought to distill our conversations and some conclusions in this report. The participants in our group who have signed on to the report, as listed on the following page, endorse "the general viewpoints and judgments reached by the group, though not necessarily every finding and recommendation." In addition to endorsing the report, some signatories elected to individually write brief statements, which appear in Appendix A.

Our participants who are currently employed full-time by government agencies are precluded from signing on because of their employment, and we simply thank them for contributing to the group discussions.

– Matt Olsen, Bruce Schneier, and Jonathan Zittrain

Project Conveners

Signatories

Urs Gasser

Nancy Gertner

Jack Goldsmith

Susan Landau

Joseph Nye

David R. O'Brien

Matthew G. Olsen

Daphna Renan

Julian Sanchez

Bruce Schneier

Larry Schwartztol

Jonathan Zittrain

Berkman

The Berkman Center for Internet & Society
at Harvard University

Don't Panic

Making Progress on the "Going Dark" Debate

February 1, 2016

Introduction

In the last year, conversations around surveillance have centered on the use of encryption in communications technologies. The decisions of Apple, Google, and other major providers of communications services and products to enable end-to-end encryption in certain applications, on smartphone operating systems, as well as default encryption of mobile devices, at the same time that terrorist groups seek to use encryption to conceal their communication from surveillance, has fueled this debate.

The U.S. intelligence and law enforcement communities view this trend with varying degrees of alarm, alleging that their interception capabilities are "going dark." As they describe it, companies are increasingly adopting technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy the Fourth Amendment's warrant requirements. Encryption is the hallmark of these architectures. Government officials are concerned because, without access to communications, they fear they may not be able to prevent terrorist attacks and investigate and prosecute criminal activity. Their solution is to force companies to maintain access to user communications and data, and provide that access to law enforcement on demand, pursuant to the applicable legal process. However, the private sector has resisted. Critics fear that architectures geared to guarantee such access would compromise the security and privacy of users around the world, while also hurting the economic viability of U.S. companies. They also dispute the degree to which the proposed solutions would truly prevent terrorists and criminals from communicating in mediums resistant to surveillance.

Leading much of the debate on behalf of the U.S. government is the Department of Justice, including the Federal Bureau of Investigation, whose leaders have commented on the matter in numerous public statements, speeches, and Congressional testimony throughout 2014 and 2015. After nearly a year of discourse, which included numerous statements critical of the government's position from former U.S. intelligence officials and security technologists, the White House declared in October 2015 it would not pursue a legislative fix in the near future.[1]

However, this decision has not brought closure. The FBI has since focused its energy on encouraging companies to voluntarily find solutions that address the investigative concerns. Most recently, terrorist attacks in San Bernardino, Paris, and elsewhere around the world, along with rising concern about the terrorist group ISIS, have focused increased attention on the issues of surveillance and encryption. These developments have led to renewed calls, including among U.S. Presidential candidates, for the government and private sector to work together on the going dark issue and for the Obama administration to reconsider its position.

Findings

Although we were not able to unanimously agree upon the scope of the problem or the policy solution that would strike the best balance, we take the warnings of the FBI and others at face value: conducting certain types of surveillance has, to some extent, become more difficult in light of technological changes. Nevertheless, we question whether the "going dark" metaphor accurately describes the state of affairs. Are we really headed to a future in which our ability to effectively surveil criminals and bad actors is impossible? We think not.

Short of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to surveillance will always exist. This is especially true given the generative nature of the modern Internet, in which new services and software can be made available without centralized vetting. However, the question we explore is the significance of this lack of access to communications for legitimate government interests. We argue that communications in the future will neither be eclipsed into darkness nor illuminated without shadow. Market forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves, and the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will "go dark" and beyond reach.

In short, our findings are:

- End-to-end encryption and other technological architectures for obscuring user data are unlikely to be adopted ubiquitously by companies, because the majority of businesses that provide communications services rely on access to user data for revenue streams and product functionality, including user data recovery should a password be forgotten.
- Software ecosystems tend to be fragmented. In order for encryption to become both widespread and comprehensive, far more coordination and standardization than currently exists would be required.
- Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel.
- Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.
- These trends raise novel questions about how we will protect individual privacy and security in the future. Today's debate is important, but for all its efforts to take account of technological trends, it is largely taking place without reference to the full picture.

A Catalyst: Apple, Google, and Others Introduce Easy-to-Use, Built-In Encryption

In September 2014, about a year and a half after the disclosures by former NSA contractor Edward Snowden, Apple announced its decision to include default encryption of the password-protected contents of its devices in the then-next version of its mobile operating systems, iOS 8.[2] Indeed, data generated by many of the system apps on iOS 8 and later versions are encrypted when data is stored locally on the phone, in transit, and stored on Apple's servers.[3] The decryption keys are tied to the device password and only stored locally on the phone.

Not long after Apple's announcement, Google followed suit by announcing that Lollipop, its next version of Android OS, would enable device encryption by default.[4] Then, in November 2014, WhatsApp, the

popular instant messaging service for smartphones now owned by Facebook, announced it would support TextSecure, an end-to-end encryption protocol.[5] In March 2015, Yahoo introduced source code for an extension that encrypts messages in Yahoo Mail, though it requires users to run a key exchange server.[6] These steps bring to the appliance-style mobile world some of the technologies that have long been available – if not enabled by default – for personal computing operating systems, such as Apple's FileVault and Microsoft's Bitlocker.

The most significant aspects of these announcements are that the encryption takes place using keys solely in the possession of the respective device holders, and it is enabled by default.

While the going dark problem encompasses a range of architectural changes that impede government access, the adoption of encryption of data at rest, and end-to-end encryption in some common communications applications, by companies has become a focal point in the current debate, particularly those in which service providers do not have access to the keys. For example, *end-to-end* encryption is being used to describe scenarios in which information is being encrypted at the end points of a communication channel, and only the original sender and intended recipient possess the keys necessary to decrypt the message. In other words, the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network between the sender and the receiver, including an intermediary service provider, such as Apple. Similarly, *device* encryption – in which the keys exist only on locked devices – prevents the contents from being read by anyone who does not possess the keys.

The distinction is important because an overwhelming percentage of Internet users communicate through web-based services, such as webmail, instant messages, and social networking websites that are not end-to-end encrypted. In the course of an investigation, government officials can intercept communications and seek access to stored communications held by these intermediaries by obtaining a warrant, court order, or subpoena, provided that the company is capable of producing the information sought. However, without access to the keys, a company like Apple is incapable of providing a means to access communications in transit or stored on the company's services, regardless of whether law enforcement presents a valid warrant or court order.[7]

The role of default options and native support for encryption is also important. As with Filevault and Bitlocker for their data at rest, individuals have been able to use encryption software to send and receive end-to-end encrypted messages for a long time. For example, the first widely available public-key crypto software, Pretty Good Privacy (PGP), was made available to the public in the early 1990s. However, for the average computer user, e-mail encryption software has proven difficult to use, especially when it is not supported natively by communication software.[8] There is a well-documented learning curve to using the

software and it adds several steps to sending messages – both the sender and the recipient need to understand the encryption process, possess the software, generate a key pair, share the public keys, and encrypt and decrypt the messages. Much of this adds complexity and friction that is simply too much for most users to bother.

The complexity is substantially reduced when encryption is supported natively by communication software. When encryption is seamlessly integrated, a user does not have to take any affirmative actions to encrypt or decrypt messages, and much of the process occurs on the back end of the software. In fact, an average user might not be able to tell the difference between an encrypted message and an unencrypted message. When these options are enabled by default on popular devices and platforms, like the iPhone, a large swath of communications is encrypted.[9] Up to this point, government officials have not had to worry about the widespread use of such encryption, but the default nature of these schemes could alter the landscape. To be sure, in the past there was simply less data for government officials to seek in the first place – the amount of digital communications taking place in the PC-only era from 1977 to 2007 – even with the rise of the Internet in between – is dwarfed by the communications facilitated by mobile devices.

Despite all the noise, few of the headline-grabbing and anxiety-provoking (for government, at least) moves by device and operating system makers from 2014 have materialized into real-world default encryption that is beyond the reach of government actors.[10] Moreover, as we explore below, for a variety of reasons, it is not clear that the wave of encryption introduced in recent years will continue.

The "Going Dark" Debate Begins (Again)

This is not the first debate about the public's ability to use encryption and the government's ability to access communications. Often recounted as the "crypto wars," government access to encrypted communications has been the subject of hot debate and restrictive policy since the 1970s, with the government ultimately relaxing many export-control restrictions on software containing strong cryptographic algorithms in 2000.[11] The roles and obligations of telecommunications companies in providing a means for government actors to wiretap voice communications – in particular on the legacy telephone system that predated the PC and Internet era – have also been debated extensively over these decades. This was framed in the U.S. by the Communications Assistance to Law Enforcement Act – CALEA – which required telephone companies and others to ensure that their networks could be wiretapped, with appropriate legal process, as network technologies moved from analog to digital.[12]

The FBI has led the government's participation in the current debate. The Bureau started publicly raising concerns in 2010 about its ability to capture online communications.[13] The FBI's then-General Counsel,

Valerie Caproni, appeared before the Senate Judiciary Committee and used the phrase "going dark" to characterize the concern, citing a widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications.[14] Her testimony emphasized that many Internet-based communications services have not only become more complex but have also deployed in modalities that are not subject to the Communications Assistance to Law Enforcement Act.[15] Other reports with similar accounts surfaced during this time period as well, including a declassified FBI situational report on cyber activity that described how data can be "hidden" from law enforcement by using encryption and the end points of communications channels can be obfuscated through use of proxies such as the Tor network.[16]

While the FBI has been the most vocal government agency about this issue,[17] foreign intelligence agencies such as the Central Intelligence Agency and National Security Agency also face obstacles due to encryption and other architectures that impede their access. The government is not a monolithic organization, and the encryption debate is not viewed the same way across governmental organizations or among the individuals within these organizations. The needs and resources of government organizations differ, as do their jurisdictional ambits. For instance, the resources available to the FBI for defeating encryption may be fewer than those available to the NSA. Likewise, state and local authorities have access to fewer resources than law enforcement operating at the federal level. However, while the degree of concern and operational value may not be shared across different agencies and levels of government, there is a general sense by actors within both the intelligence and law enforcement communities that, were all else equal, they would benefit if technological architectures did not present a barrier to investigations. (To be sure, all else is not equal – for example, if all communications were routinely unencrypted, citizens would be exposed to surveillance from myriad sources, many of whom might be viewed as national security threats by those citizens' governments.) Meanwhile certain agencies, including the Department of State, the Naval Research Laboratories, and the Defense Advanced Research Projects Agency (DARPA) have helped support the development of the Tor network, which hides the transactional information of Web-based communications. There are security reasons as well as human-rights interests for the U.S. government's support of Tor.

Since Caproni's invocation of the going dark metaphor in 2010, the problem, according to government officials, continues to worsen. Encryption has become central to their concerns. FBI Director James Comey, who has perhaps been the most vocal government official on this topic throughout the last year, highlighted his unease in October 2014 shortly after the announcements from Apple and Google:

> "Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."[18]

In other public statements and Congressional testimony, Director Comey and others, including Deputy Attorney General Sally Yates, have continued to call attention to the problem. According to these statements, the going dark problem is being fueled by "the advent of default encryption settings and stronger encryption standards on both devices and networks,"[19] and, it may have a number of implications. For instance, according to FBI officials, "if there is no way to access the data . . . we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets."[20]

According to government officials, use of encryption may inhibit the ability of law enforcement and the intelligence community to investigate and prevent terrorist attacks. More specifically, Director Comey has stated that ISIS operators in Syria are "recruiting and tasking dozens of troubled Americans to kill people, [using] a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment."[21] FBI officials have also emphasized that the FBI does not possess the capability to defeat encryption using brute-force attacks and there is not an easy way to get around strong encryption.[22] Recently, Director Comey in Congressional testimony identified a terrorist attack in Garland, Texas, as an example: "[B]efore one of those terrorists left and tried to commit mass murder, he exchanged 109 messages with an overseas terrorist," Comey told a Senate committee. "We have no idea what he said, because those messages were encrypted."[23]

Others from the U.S. intelligence and law enforcement community, including NSA Director Admiral Michael Rogers, Homeland Security Secretary Jeh Johnson, and Attorney General Loretta Lynch have also voiced concerns about the going dark problem.[24] In the wake of the November 2015 ISIS-associated attacks in Paris, even in the absence of an on-the-record assertion that the terrorists used encryption to protect their communications, Central Intelligence Agency Director John Brennan suggested terrorists' use of technology "make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it."[25] Whatever the assessment of the use of

encrypted communications to frustrate government investigations, a number of former officials from law enforcement and the intelligence community have disagreed about the need for a policy intervention.[26]

Although much of the debate in the media has focused on whether Director Comey is asking for companies like Google and Apple to preserve access to user data, no formal proposals have emerged from the FBI or other members of the law enforcement and intelligence communities. In July 2015, Director Comey noted in an appearance before the Senate Judiciary and House Intelligence Committees that "while there has not yet been a decision whether to seek legislation, we must work with Congress, industry academics, privacy groups, and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months."[27] Director Comey has also called on the private sector for help in identifying solutions that provide the public with security without frustrating lawful surveillance efforts. Most recently, in October 2015, Comey confirmed in testimony that the Obama administration will not, for the time being, pursue a legislative mandate, but will instead "continue conversations with industry" to find voluntary solutions.[28]

Similar debates are ongoing in other countries.[29] In the United Kingdom, Prime Minister David Cameron proposed an outright ban on end-to-end encryption technologies following the January 2015 attacks at the *Charlie Hebdo* offices in Paris.[30] The more recent November attacks in Paris have also caused French authorities to question policies surrounding the availability of encryption software.[31] Other European countries have passed or are considering legislation that would require companies to retain readable user data and provide access to government authorities on request.[32] And nation states that recognize fewer constitutional or other legal barriers to generating government demands for data, such as Saudi Arabia, Russia, and the U.A.E., have pioneered the use of pre-emptive legal mandates for data retention and decryption by technology providers.

Before we delve into the issues with the going dark metaphor, a few general observations are worth highlighting in brief.

The debate brings to the fore a number of tensions between security, privacy, economic competitiveness, and government access to information. A rich trove of expert literature explores these issues in detail.[33] Many of the technical and political merits of the debate were the focus of the recently published *Keys Under Doormats* report, authored by several of those who join this paper.[34] While these perspectives are out of scope for this paper, we acknowledge their importance for understanding the many dimensions of the going dark debate.

The global stage on which this debate is unfolding is worth emphasizing. Many geopolitical partners to the U.S. are actively engaged in discussions about promoting cybersecurity and the appropriate limits of surveillance across borders. For instance, the U.S.-E.U. Data Protection safe harbor, which provided a legal framework since the turn of the century for commercial cross-border data flows, was recently ruled invalid by the Court of Justice of the European Union due to concerns about the U.S. intelligence community's ability to access data.[35] The U.N. has also weighed in to a limited extent on encryption, recently declaring it "necessary for the exercise of the right to freedom of expression."[36]

Meanwhile, many U.S. companies must also answer to governments of foreign countries in which they do business. In this vein, they are increasingly playing a quasi-sovereign role as they face difficult decisions when foreign government agencies pressure them to produce data about citizens abroad. Many companies refuse to change the architecture of their services to allow such surveillance. However, if the U.S. government were to mandate architectural changes, surveillance would be made easier for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents. The comparatively well-developed legal doctrines, procedural requirements, and redress mechanisms that serve as backstops to the U.S. government's surveillance activities are not mirrored worldwide.

On the subject of surveillance tools and techniques, much has changed over the past twenty years. The digital revolution has proven to be a boon for surveillance – it has become possible to track and learn about individuals at very granular level.[37] Although use of encryption may present a barrier to surveillance, it may not be impermeable. There are many ways to implement encryption incorrectly and other weaknesses beyond encryption that are exploitable.[38] For example, encryption does not prevent intrusions at the end points, which has increasingly become a technique used in law enforcement investigations.[39] Encryption typically does not protect metadata, such as e-mail addresses and mobile-device location information, that must remain in plaintext to serve a functional purpose. Data can also be leaked into unencrypted media, through cloud backups and syncing across multiple devices.[40]

Going Dark is the Wrong Metaphor

The going dark metaphor suggests that communications are becoming steadily out of reach – an aperture is closing, and once closed we are blind. This does not capture the current state and trajectory of technological development.

To be sure, encryption and provider-opaque services make surveillance more difficult in certain cases, but the landscape is far more variegated than the metaphor suggests. There are and will always be pockets of

dimness and some dark spots – communications channels resistant to surveillance – but this does not mean we are completely "going dark." Some areas are more illuminated now than in the past and others are brightening. Three trends in particular facilitate government access. First, many companies' business models rely on access to user data. Second, products are increasingly being offered as services, and architectures have become more centralized through cloud computing and data centers. A service, which entails an ongoing relationship between vendor and user, lends itself much more to monitoring and control than a product, where a technology is purchased once and then used without further vendor interaction. Finally, the Internet of Things promises a new frontier for networking objects, machines, and environments in ways that we just beginning to understand. When, say, a television has a microphone and a network connection, and is reprogrammable by its vendor, it could be used to listen in to one side of a telephone conversation taking place in its room – no matter how encrypted the telephone service itself might be. These forces are on a trajectory towards a future with more opportunities for surveillance.

In this section, we hope to elucidate this counter narrative. We do not suggest that the problem the FBI and others have identified is necessarily solved by the availability of other sources of data, nor do we conflate availability with the government's ability to gain access. Rather, we think that the forces opening new opportunities for government surveillance mean that, whatever the situation with iOS 8 encryption versus its predecessor, "going dark" does not aptly describe the long-term landscape for government surveillance. Any debate about surveillance capabilities today that will result in lasting policy should take into account these larger trends.

Encryption Runs Counter to the Business Interests of Many Companies

Current company business models discourage implementation of end-to-end encryption and other technological impediments to company, and therefore government, access.

For the past fifteen years, consumer-facing Internet companies have relied on advertising as their dominant business model. Ads are frequently used to subsidize free content and services. Internet companies more recently have been shifting towards data-driven advertising, and the technology that facilitates advertising delivery has become more reliant on user data for targeting ads based on demographics and behaviors. Companies seek to make behavioral assessments to match ads to individuals on the fly. Google products display advertising determined by behavioral patterns, search queries, and other signals collected by Google.[41] Similarly, Facebook claims it is capable of reaching narrow audiences in advertising campaigns with "89% accuracy" based on location, demographics, interests, and behaviors.[42] Yahoo products are also supported by advertising.[43] And, the list goes on.

To fuel this lucrative market, companies typically wish to have unencumbered access to user data – with privacy assured through either restricting dissemination of identifiable customer information outside the boundaries of the company (and of governments, should they lawfully request the data). Implementing end-to-end encryption by default for all, or even most, user data streams would conflict with the advertising model and presumably curtail revenues. Market trends so far reflect that companies have little incentive to veer from this model, making it unlikely that end-to-end encryption will become ubiquitous across applications and services. As a result, many Internet companies will continue to have the ability to respond to government orders to provide access to communications of users.

Cloud computing entails the movement of data and software to centralized locations operated by companies instead of under direct user custody. This technology, made possible by ubiquitous connectivity, enables businesses and individuals to extend their computing resources through the Internet at remote data centers, much like a utility service.[44] As a result, products are increasingly being offered as services, which in turn marks a shift away from traditional notions of ownership and control, and more towards centralized repositories of user data. Software and data no longer need to be installed and stored locally on an individual's computer – they can be delivered through a cloud service (e.g., Google Apps) or stored remotely in a cloud storage service (e.g., Dropbox) where they can be conveniently accessed from anywhere through a web browser or a smartphone app.[45] Webmail, social networking, word processing, and other common applications are now typically delivered as networked services.[46] These services deliver substantial benefits and convenience to both individuals and companies, and they are often provided free in ad-subsidized models or in economical pay-as-you-go arrangements.[47]

End-to-end encryption is currently impractical for companies who need to offer features in cloud services that require access to plaintext data. For example, Google offers a number of features in its web-based services that require access to plaintext data, including full text search of documents and files stored in the cloud. In order for such features to work, Google must have access to the plaintext. While Apple says that it encrypts communications end-to-end in some apps it develops, the encryption does not extend to all of its services. This includes, in particular, the iCloud backup service, which conveniently enables users to recover their data from Apple servers. iCloud is enabled by default on Apple devices. Although Apple does encrypt iCloud backups,[48] it holds the keys so that users who have lost everything are not left without recourse. So while the data may be protected from outside attackers, it is still capable of being decrypted by Apple.[49] Since Apple holds the keys, it can be compelled through legal process to produce user data that resides in iCloud.

There are a number of other reasons why a shift to encryption or other architectures would not appeal to businesses. Encryption schemes often add complexity to the user experience. Former Facebook Chief Security Officer Joe Sullivan observed that Facebook "has been able to deploy end-to-end encryption for a long time," but it has held back due to the added complexity and because "when end-to-end encryption is done right, it's hard for the average person to communicate."[50] Google has also reportedly held off on implementing device encryption by default on locked Android devices due to performance issues, despite its announcements that it would do so in 2014.[51] To date, the latest version of Android does not enable encryption by default.

Fragmentation in software ecosystems can also impede the degree to which new conventions and architectural changes – especially those that would enable user-to-user encryption across different devices and services – become widespread. In these ecosystems, multiple points of control may exist that influence the types of apps and operating system updates that eventually filter down to end users.

For example, in the Android ecosystem, smartphones are controlled by the wireless providers and handset manufacturers who create customized versions of the Android operating systems for the phones they sell. These companies have little incentive to update older phones to the latest versions of Android, because it would require them to invest resources into making the customized features compatible with newer versions of Android.[52] In fact, many older Android smartphones are never updated to newer OS versions. According to Google, as of this writing, approximately 32% of Android devices are running the latest Lollipop, which was released in November 2014.[53] In addition, although the next version of Android released by Google may contain apps that support end-to-end encryption, a manufacturer or wireless provider may modify the software to include its own suite of custom apps that do not support encryption. Some of these companies may have commercial interests in retaining access to plaintext communications.[54] A wide variety of third-party messaging applications are also available on Google Play, and end users can install and use them in place of the pre-installed messaging app that ships on their phones. In order for end-to-end encryption to work properly, both a sender's and receiver's messaging apps must be able to support it, and not all do. If the ecosystem is fragmented, encryption is that much less likely to become all encompassing.

The Internet of Things and Networked Sensors Open Uncharted Paths to Surveillance

A plethora of networked sensors are now embedded in everyday objects. These are prime mechanisms for surveillance: alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become. To paint an overall picture of going dark

based upon the fact that a number of widely used applications and products have introduced encryption by default risks obscuring this larger trend.

According to analysts and commentators representing the conventional wisdom, the Internet of Things (IoT) is the next revolution in computing. Expert observers have suggested that "the Internet of Things has the potential to fundamentally shift the way we interact with our surroundings," at work, at home, in retail environments, in cars, and on public streets.[55] The IoT market is forecast to grow into a multi-trillion dollar industry within the next ten years,[56] and according to a survey of experts, it will have "widespread and beneficial effects by 2025."[57] This will result in significant changes in how members of society interact with one another and the inanimate objects around them.[58]

Appliances and products ranging from televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches and other wearables are being packed with sensors and wireless connectivity.[59] Numerous companies are developing platforms and products in these areas.[60] To name but a few, Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products with embedded IoT functionality, with sensors ranging from gyroscopes, accelerometers, magnetometers, proximity sensors, microphones, speakers, barometers, infrared sensors, fingerprint readers, and radio frequency antennae with the purpose of sensing, collecting, storing, and analyzing fine-grained information about their surrounding environments. These devices will all be connected to each other via the Internet, transmitting telemetry data to their respective vendors in the cloud for processing.[61]

The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications. A ten-year-old case involving an in-automobile concierge system provides an early indication of how this might play out. The system enables the company to remotely monitor and respond to a car's occupants through a variety of sensors and a cellular connection. At the touch of a button, a driver can speak to a representative who can provide directions or diagnose problems with the car. During the course of an investigation, the FBI sought to use the microphone in a car equipped with such a system to capture conversations taking place in the car's cabin between two alleged senior members of organized crime. In 2001, a federal court in Nevada issued *ex parte* orders that required the company to assist the FBI with the intercept. The company appealed, and though the Ninth Circuit disallowed the interception on other grounds, it left open the possibility of using in-car communication devices for surveillance provided the systems' safety features are not disabled in the process.[62] Such assistance might today be demanded from any company capable of recording conversations or other activity at a distance, whether through one's own smartphone, an Amazon Echo, a

baby monitor, an Internet-enabled security camera, or a futuristic "Elf on a Shelf" laden with networked audio and image sensors.[63]

In February 2015, stories surfaced that Samsung smart televisions were listening to conversations through an onboard microphone and relaying them back to Samsung to automatically discern whether owners were attempting to give instructions to the TV.[64] A statement published in Samsung's privacy policy instructed users to "be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of the Voice Recognition."[65]

Any given step of Samsung's process makes sense to offer the TV's features. Voice recognition is a computationally intensive task, and the processing capabilities of a modern television would be insufficient to make such a feature work. This is a common challenge for IoT devices that have limited processing power and limited battery capacity. The solution, in this case, was to utilize cloud infrastructure through a network connection to send the voice data to a remote server for processing and interpretations of that data back to the television as machine-actionable commands. Simple commands, such as "switch to channel 13," could be processed locally, but more complex ones, such as "show me a sci-fi movie like last week's, but not with Jane Fonda," would need to be sent to the cloud infrastructure – and in Samsung's case, to a third party, for processing.

Similarly, Google's Chrome browsing software supports voice commands using the onboard microphone in a laptop or desktop computer. The feature is activated when a user states the phrase "OK Google," and the resource intensive voice processing takes place on Google's remote servers.[66] Even children's toys are beginning to possess these features. In April 2015, Mattel introduced "Hello Barbie," an interactive doll capable of responsive speech, which is accomplished by recording children's interactions with the doll through a microphone, processing it in the cloud, and sending verbal responses through a speaker on the doll.[67] IP video cameras have also risen in popularity in the last several years. Devices like the Nest Cam record high resolution video with a wide-angle lens camera broadcast over the Internet to account holders.[68] Users can tune into the recording from Nest's website or through an app on their phone, and a camera will send an alert if it detects motion or an unusual noise. The Nest Cam can also exchange data and interact with other devices, such as Nest's thermostats and smoke detectors, which themselves contain sensors and microphones.

Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target. These are all real products now. If the Internet of Things has as

much impact as is predicted, the future will be even more laden with sensors that can be commandeered for law enforcement surveillance; and this is a world far apart from one in which opportunities for surveillance have gone dark. It is vital to appreciate these trends and to make thoughtful decisions about how pervasively open to surveillance we think our built environments should be – by home and foreign governments, and by the companies who offer the products that are transforming our personal spaces.

Concluding Thoughts

The debate over encryption raises difficult questions about security and privacy. From the national security perspective, we must consider whether providing access to encrypted communications to help prevent terrorism and investigate crime would also increase our vulnerability to cyber espionage and other threats, and whether nations that do not embrace the rule of law would be able to exploit the same access. At the same time, from a civil liberties perspective, we must consider whether preventing the government from gaining access to communications under circumstances that meet Fourth Amendment and statutory standards strike the right balance between privacy and security, particularly when terrorists and criminals seek to use encryption to evade government surveillance.

In examining these questions, our group focused on the trajectory of surveillance and technology. We concluded that the "going dark" metaphor does not fully describe the future of the government's capacity to access the communications of suspected terrorists and criminals. The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities. However, we concluded that the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information from surveillance.

Looking forward, the prevalence of network sensors and the Internet of Things raises new and difficult questions about privacy over the long term. This means we should be thinking now about the responsibilities of companies building new technologies, and about new operational procedures and rules to help the law enforcement and intelligence communities navigate the thicket of issues that will surely accompany these trends.

Appendix A: Individual Statements from Signatories

Three signatories to this report elected to write statements to individually reflect on the report or particular issues discussed within it. The statements listed below are included in this Appendix.

Susan Landau, "The National-Security Needs for Ubiquitous Encryption"

Bruce Schneier, "Security or Surveillance?"

Jonathan Zittrain, "The Good News and the Troubling News: We're not going dark"

The National-Security Needs for Ubiquitous Encryption

Susan Landau

Each terrorist attack grabs headlines, but the insidious theft of U.S. intellectual property – software, business plans, designs for airplanes, automobiles, pharmaceuticals, etc. – by other nations does not. The latter is the real national-security threat and a strong reason for national policy to favor ubiquitous use of encryption.

In 2000, the U.S. government loosened export controls on encryption. In part this was because of pressures from Silicon Valley and Congress,[1] but in large part, the reason for this change was national security. The end of the Cold War led to a temporary decline in military spending. One way to accommodate the shift was to turn to commercial off the shelf (COTS) equipment, a requirement formalized in the 1996 Clinger-Cohen Act.[2] Another reason for the shift to COTS equipment for communications and computer technology was the speed of innovation in Silicon Valley. The need for ubiquitous security throughout our communications systems represented the third major reason.

There was an era when Blackberrys were the communication device of choice for the corporate world; these devices, unlike the recent iPhones and Androids, can provide cleartext of the communications to the phone's owner (the corporation for whom the user works). Thus businesses favored Blackberrys.

But apps drive the phone business. With the introduction of iPhones and Androids, consumers voted with their hands. People don't like to carry two devices, and users choose to use a single consumer device for *all* communications. We have moved to a world of BYOD (Bring Your Own Device).[3] In some instances, e.g., jobs in certain government agencies, finance, and the Defense Industrial Base, the workplace can require that work communications occur only over approved devices. But such control is largely ineffective in most work situations. So instead of Research in Motion developing a large consumer user base, the company lost market share as employees forced businesses to accept their use of personal

---

[1] For a longer explanation of the confluence of issues, *see, e.g.*, Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st" in Karl De Leeuw and Jan Bergstra (eds.), *The History of Information Security* (Elsevier, 2007), at 733-735.

[2] 40 U.S.C. § 1401 *et seq*.

[3] Mick Slattery, "How Consumer Technology is Remaking the Workplace," *WIRED*, March 2013, http://www.wired.com/insights/2013/03/how-consumer-technology-is-remaking-the-workplace/.

devices for corporate communications. Thus access to U.S. intellectual property lies not only on corporate servers – which may or may not be well protected – but on millions of private communication devices.

Protecting U.S. intellectual property is crucial for U.S. economic and national security, and given BYOD – a social change that is here to stay – encrypted communications are necessary for national security. In a July 2015 *Washington Post* op-ed former DHS Secretary Michael Chertoff, former NSA Director Mike McConnell, and former Deputy Defense Secretary William Lynn concurred, observing that "Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interest. . . . If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential."[4] They concluded that the security provided by encrypted communications was more important than the difficulties encryption present to law enforcement.

There are, after all, other ways of going after communications content than providing law enforcement with "exceptional access" to encrypted communications. These include using the existing vulnerabilities present in the apps and systems of the devices themselves. While such an approach makes investigations more expensive, this approach is a tradeoff enabling the vast majority of communications to be far more secure.

Exceptional access is dangerous. As my co-authors and I have described in our *Keys under Doormats* paper,[5] proposals for law-enforcement "exceptional access" ignore the realities of current software. Getting software correct is very difficult. Thus, for example, when NSA tested CALEA-compliant switches,[6] it discovered security problems with every implementation.[7] Furthermore, exceptional access

---

[4] Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear of ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

[5] Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

[6] The 1994 Communications Assistance for Law Enforcement Act (CALEA) requires all digitally switched networks be built to accommodate lawful surveillance. Pub. L. 103-414.

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

prevents the deployment of two extremely useful forms of security: forward secrecy and authenticated encryption.[8]

At a time when nation-state espionage is heavily aimed at business communications and these communications are often found on personal devices, national security dictates that they be secured. And that means policy facilitating the ubiquitous use of uncompromised strong encryption is in our national security interest.

[8] Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

Security or Surveillance?

Bruce Schneier

Both the "going dark" metaphor of FBI Director James Comey[1] and the contrasting "golden age of surveillance" metaphor of privacy law professor Peter Swire[2] focus on the value of data to law enforcement. As framed in the media, encryption debates are about whether law enforcement should have surreptitious access to data, or whether companies should be allowed to provide strong encryption to their customers.

It's a myopic framing that focuses only on one threat – criminals, including domestic terrorists – and the demands of law enforcement and national intelligence. This obscures the most important aspects of the encryption issue: the security it provides against a much wider variety of threats.

Encryption secures our data and communications against eavesdroppers like criminals, foreign governments, and terrorists. We use it every day to hide our cell phone conversations from eavesdroppers, and to hide our Internet purchasing from credit card thieves. Dissidents in China and many other countries use it to avoid arrest. It's a vital tool for journalists to communicate with their sources, for NGOs to protect their work in repressive countries, and for attorneys to communicate with their clients.

Many technological security failures of today can be traced to failures of encryption. In 2014 and 2015, unnamed hackers – probably the Chinese government – stole 21.5 million personal files of U.S. government employees and others. They wouldn't have obtained this data if it had been encrypted. Many large-scale criminal data thefts were made either easier or more damaging because data wasn't encrypted: Target, TJ Maxx, Heartland Payment Systems, and so on. Many countries are eavesdropping on the unencrypted communications of their own citizens, looking for dissidents and other voices they want to silence.

---

[1] James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course," speech at Brookings Institution, October 16, 2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[2] Peter Swire, testimony at Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," July 8, 2015. https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

Adding backdoors will only exacerbate the risks. As technologists, we can't build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document.[3] If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists. This is not theoretical; again and again, backdoor accesses built for one purpose have been surreptitiously used for another. Vodafone built backdoor access into Greece's cell phone network for the Greek government; it was used against the Greek government in 2004-2005.[4] Google kept a database of backdoor accesses provided to the U.S. government under CALEA; the Chinese breached that database in 2009.[5]

We're not being asked to choose between security and privacy. We're being asked to choose between less security and more security.

This trade-off isn't new. In the mid-1990s, cryptographers argued that escrowing encryption keys with central authorities would weaken security.[6] In 2011, cybersecurity researcher Susan Landau published her excellent book *Surveillance or Security?*, which deftly parsed the details of this trade-off and concluded that security is far more important.[7]

Ubiquitous encryption protects us much more from bulk surveillance than from targeted surveillance. For a variety of technical reasons, computer security is extraordinarily weak. If a sufficiently skilled, funded, and motivated attacker wants in to your computer, they're in. If they're not, it's because you're not high enough on their priority list to bother with. Widespread encryption forces the listener – whether a foreign government, criminal, or terrorist – to target. And this hurts repressive governments much more than it hurts terrorists and criminals.

---

[3] Hal Abelson et al., "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

[4] Vassilis Prevelakis, Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, June 27, 2007. http://spectrum.ieee.org/telecom/security/the-athens-affair.

[5] Ellen Nakashima, "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 20, 2013, https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[6] Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1998. https://www.schneier.com/paper-key-escrow.html.

[7] Susan Landau, Surveillance or Security: The Risks Posed by New Wiretapping Technologies (Cambridge: MIT Press, 2011).

Of course, criminals and terrorists have used, are using, and will use encryption to hide their planning from the authorities, just as they will use many aspects of society's capabilities and infrastructure: cars, restaurants, telecommunications. In general, we recognize that such things can be used by both honest and dishonest people. Society thrives nonetheless because the honest so outnumber the dishonest. Compare this with the tactic of secretly poisoning all the food at a restaurant. Yes, we might get lucky and poison a terrorist before he strikes, but we'll harm all the innocent customers in the process. Weakening encryption for everyone is harmful in exactly the same way.

The Good News and the Troubling News: We're not going dark

Jonathan Zittrain

Two trends have dominated the U.S. foreign intelligence landscape for the past fifteen years.

The first arises from the terrorist attacks of 9/11. The attacks reshaped the priorities of the U.S. intelligence community, as extraordinary resources have been allocated to prevent and counter terrorism. Our national security establishment has pioneered new technological tools and new legal authorities (or interpretations of existing ones) in an effort to secure safety.

The second trend is the mainstreaming of the Internet and surrounding technologies built around and upon it, which has led to an unprecedented proliferation of data that can be analyzed by the intelligence services. In late 2001 there were no smartphones and no social media. Facebook and Twitter were still years away from capturing our imagination, our time – and our data. The more bits we generate, actively through typing and talking, and passively by sharing our location, our social relationships, and other information as we go about our lives, the more there is for vendors – and the governments to whom they answer – to potentially review, whether in bulk or individually.

The intersection of these trends led to what Peter Swire and Kenesa Ahmad in 2011 called "the Golden Age of Surveillance."[1] Since then, that high water mark for opportunities for surveillance has receded in places. Some communications and data previously accessible by governments through vendors is no longer so easily obtained, because some vendors have refined the technologies they offer to prevent even themselves from seeing the data the users generate and exchange with one another. Such technologies, including the use of encryption, are not new as a category, but their entry into mainstream usage perhaps is. Losing a tool, rather than never having had it to begin with, is no doubt highly salient for the director of the FBI and others charged with protecting security. They ask: if we have a warrant or other legal authority, why should previously-accessible information now be off-limits to us?

I empathize with the idea that just how much government can learn about us should not depend on the cat and mouse game of technological measure and counter-measure. Ideally, a polity would carefully calibrate its legal authorities to permit access exactly and only where it comports with the imperatives of

[1] Peter Swire and Kenesa Ahmad, "'Going Dark' Versus a Golden Age of Surveillance," Center for Democracy & Technology, November 28, 2011.

legitimate security – and with basic human rights as recognized through the protections of conventions and constitutions. For one intriguing attempt to reconcile government use of technological hacking tools with appropriate privacy protections, you might read the proposal for "lawful hacking" that civil liberties-minded computer scientists Steven Bellovin, Matt Blaze, Sandy Clark, and fellow project participant Susan Landau have advocated.[2]

But it is a very large step – a leap, even – to go beyond the legal demand for information already in a company's possession, and beyond the use of technological tools to reveal what otherwise is obscure, to requirements on how technology must be deployed to begin with. I've written reasons why this leap is ill-advised.[3] To try to constrain the generative Internet ecosystem in that way would be either futile or require that we, in the fitting words of the U.S. Supreme Court, "burn the house to roast the pig."[4] That turn of phrase was used by Justice Frankfurter to explain why a Michigan law banning books that could tend to "corruption of the morals of youth" violated the First Amendment, even if it was aimed at a laudable goal. Here, too, there are times we will rue the cleverness or luck of a criminal who benefits first from the Internet's facilitation of communication and organization, and then from encryption to prevent his or her activities from being discovered or investigated. But this is not reason enough to require that foundational technologies be restricted or eliminated in general use – any more than the population of Michigan could rightly be restricted to reading only what is fit for children.

Most of the "Don't Panic" report from our Berklett cybersecurity project isn't about that. Given the spectrum of roles and viewpoints represented in the room, our focus was more on a factual (if speculative) question – are we really "going dark"? – than one of articulating and balancing values. The answer, in the big picture, is no, even as it's small solace to a prosecutor holding both a warrant and an iPhone with a password that can't be readily cracked. (To be sure, many of those situations will also have an owner who could, after process, be ordered by a court to unlock the phone on pain of contempt.)

---

[2] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," 12 *Northwestern Journal of Technology & Intellectual Property* 1 (2014), available at http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.

[3] *See* Jonathan Zittrain, "An Open Letter to Prime Minister Cameron: 20th-Century Solutions Won't Help 21st-Century Surveillance," (2015), https://medium.com/message/dear-prime-minister-cameron-20th-century-solutions-wont-help-21st-century-surveillance-ff2d7a3d300c.

[4] *Butler v. Michigan*, 352 U.S. 380, 383 (1957).

As data collection volume and methods proliferate, the number of human and technical weaknesses within the system will increase to the point that it will overwhelmingly likely be a net positive for the intelligence community. Consider all those IoT devices with their sensors and poorly updated firmware. We're hardly going dark when – fittingly, given the metaphor – our light bulbs have motion detectors and an open port. The label is "going dark" only because the security state is losing something that it fleetingly had access to, not because it is all of a sudden lacking in vectors for useful information.

But exactly what should reassure government officials, and stay the momentum for major policy interventions into Internet technology development, is what should also trouble everyone: we are hurtling towards a world in which a truly staggering amount of data will be only a warrant or a subpoena away, and in many jurisdictions, even that gap need not be traversed. That's why this report and the deliberations behind it are genuinely only a beginning, and there's much more work to do before the future is upon us.

Appendix B: Berklett Cybersecurity Project Group Members and Guests

More information about the Berkman Center's Berklett Cybersecurity Project can be found here: http://brk.mn/cybersecurity.

At the heart of the project is an extremely diverse group of experts who regularly convene, approximately every three months, to discuss enduring problems of surveillance and cybersecurity. As part of the meetings, special guests are occasionally invited to join these meetings for the opportunity to share unique perspectives on specific topics of discussion.

The core members of the group are:[*]

> **John DeLong:** the Director of the Commercial Solutions Center at the National Security Agency. Formerly he was the Director of Compliance at the NSA and previously served as the Deputy Director of the National Cyber Security Division at the Department of Homeland Security. He has also developed classes and taught at the National Cryptologic School in areas of compliance, computer science, and cybersecurity.
>
> **Urs Gasser:** the Executive Director of the Berkman Center for Internet & Society and a Professor of Practice at Harvard Law School. His research includes activities focused on information law, policy, and society with projects in collaboration with leading international research institutions exploring regulation, ICT interoperability, cybersecurity, and the law's impact on innovation and risk in the ICT space. Urs is the author of several books, including, with John Palfrey, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books, 2012).
>
> **Hon. Nancy Gertner (ret.):** a former U.S. federal judge for the U.S. District Court for the District of Massachusetts. She was appointed to the federal bench by President Bill Clinton in 1994,

---

[*] This publication would not have been possible without contributions from the project's talented team members and collaborators, in particular Samantha Bates, Tiffany Lin, Shailin Thomas, and Jordi Weinstock, who contributed research, editing, and inspiration throughout the writing process. A number of the Berkman Center's summer interns, research assistants, and Harvard Law School students also contributed to the report, including Abby Colella, David Eichert, Lydia Lichlyter, and Grant Nelson. We are also indebted to many other staff members at the Center and Harvard Law School who supported the project and the report, including Carey Andersen, Ryan Budish, Rob Faris, Dan Jones, Sue Kriegsman, Amanda McMahan, Annie Pruitt, Daniel Oyolu, Gretchen Weber, and Amy Zhang.

holding the position for 17 years. She has written and spoken widely on various legal issues concerning civil rights and liberties, criminal justice, and procedural issues. Currently, she is a Senior Lecturer on Law at Harvard Law School.

Jack Goldsmith: formerly served as Assistant Attorney General, Office of Legal Counsel, and Special Counsel to the Department of Defense for the Bush Administration. He is the Henry L. Shattuck Professor of Law at Harvard Law School and a Senior Fellow at the Hoover Institution at Stanford University. He is also the co-founder of Lawfareblog.com, and focuses on national security, international, and Internet law, and cybersecurity.

Susan Landau: a professor of cybersecurity policy at Worcester Polytechnic Institute and a visiting professor in computer science at University College London. She works at the intersection of cybersecurity, national security, law, and policy, and is the author of numerous books, including *Surveillance or Security?: Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and, with Whitfield Diffie, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, rev. ed. 2007). Susan has previously served as a senior staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems.

Anne Neuberger: the Chief Risk Officer at the National Security Agency, responsible for the implementation of the risk management process. She is also a member of the NSA's Senior Leadership team. Previously she served as the Director of NSA's Commercial Solutions Center, and as Special Assistant to the Director for the Enduring Security Framework.

Joseph Nye: formerly served as the Assistant Secretary of Defense for International Security Affairs, Chair of the National Intelligence Council, and was the Deputy Under Secretary of State for Security Assistance, Science and Technology. Ranked as the most influential scholar on American foreign policy, he has written extensively on international relations and power. He was formerly the Dean of the Harvard Kennedy School of Government and is currently a University Distinguished Service Professor at Harvard.

David R. O'Brien: a Senior Researcher at the Berkman Center for Internet & Society at Harvard University, where he leads research initiatives on privacy and cybersecurity. He formerly practiced intellectual property and technology law in Boston.

Matthew G. Olsen: former Director of the U.S. National Counterterrorism Center appointed by President Obama in 2011. Prior to that position, he served as General Counsel for the National Security Agency, in leadership positions at the Department of Justice, and as a federal prosecutor. Currently, he is a president and co-founder of IronNet Cybersecurity, a lecturer at Harvard Law School, and a national security analyst for ABC News.

Daphna Renan: served as an Attorney Advisor in the Justice Department's Office of Legal Counsel as well as Counsel to the Deputy Attorney General. She is currently an Assistant Professor of Law at Harvard Law School where her research examines surveillance as ongoing and routinized domestic administration, and explores mechanisms for its systematic governance.

Julian Sanchez: a Senior Fellow at the Cato Institute who studies technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance. He was formerly the Washington editor for Ars Technica, and was a writer for The Economist's Democracy in America. He is also a founding editor of the policy blog, Just Security.

Bruce Schneier: a renowned security technologist who has written extensively on security issues, both academically and within the public. He is the Chief Technology Officer of Resilient Systems, a fellow at the Berkman Center for Internet & Society, a program fellow at the Open Technology Institute, and a board member of the Electronic Frontier Foundation. He is also the author of numerous books on security, surveillance, and cryptography, including the New York Times Bestseller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton and Company, 2015).

Larry Schwartztol: formerly worked as a staff attorney at the American Civil Liberties Union's National Security project, litigating cases involving foreign intelligence surveillance. He was also a staff attorney in the ACLU's Racial Justice Program, litigating cases at the intersection of racial and economic justice. He is currently the executive director of the Criminal Justice Program of Study, Research & Advocacy at Harvard Law School.

Jonathan Zittrain: is the George Bemis Professor of International Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and co-founder and Faculty Director of the Berkman Center for Internet & Society. He is a member of the Board of Directors of the Electronic Frontier Foundation and also contributes to the advisory board of the National Security Agency.

Meeting guests have included:

James Baker, Federal Bureau of Investigation

James Burell, Federal Bureau of Investigation

Janice Gardner, Office of the Director of National Intelligence

Melissa Hathaway, Harvard Kennedy School's Belfer Center; Hathaway Global Strategies

Eli Sugarman, William and Flora Hewlett Foundation

Ben Wittes, Lawfare; Brookings Institution

---

[1] *See* Ellen Nakashima and Andrea Peterson, "Obama administration opts not to force firms to decrypt data – for now," *The Washington Post*, October 8, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[2] David Sanger, "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *The New York Times*, September 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

[2] Apple, Inc., "iOS Security Guide: iOS 8.1 or later," October 2014.

[3] *Ibid.*

[4] Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[5] Andy Greenberg, "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," *WIRED*, November 18, 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

[6] Alex Stamos, "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail," *Yahoo Blog*, March 15, 2015, http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption.

[6] Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *The New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[7] *See* filings related to *In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*, No. 15-MC-1902 (EDNY October 9, 2015).

[8] Alma Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in Lori Cranor and Simpson Garfinkel, *Security and Usability: Designing Systems that People Can Use* (O'Reilly: Sebastapol, 2005).

[9] In early 2014, more than 600 million individuals worldwide were estimated to use iPhones and more than 1.9 billion individuals were estimated to use phones running Android. *See* Dawiderpal Sahota, "Android Domination to continue in 2014; iPhone loses ground," *Telecoms.com*, January 2014, http://telecoms.com/210391/android-domination-to-continue-in-2014-iphone-loses-ground/.

[10] *See*, *e.g.*, Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," *MIT Technology Review*, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark; Jan Willem Aldershoff, "Users shouldn't trust WhatsApp's end-to-end encryption," MYCE.com, May 1, 2015, http://www.myce.com/news/users-shouldnt-trust-on-whatsapps-end-to-end-encryption-75939/.

[11] For a thorough history, *see* Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press: Cambridge, 2007).

[12] *See* Ben Adida, Collin Anderson, Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints," (May 17, 2013).
[13] Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *The New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.
[14] "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," Before the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, United States House of Representatives, 112th Cong. (2011), http://judiciary.house.gov/_files/hearings/printers/112th/112-59_64581.PDF.
[15] Enacted in 1994, CALEA required require telecommunications companies to modify their digital infrastructure so that law enforcement agencies would be able to conduct lawful surveillance activities. Pub. L. 103-414, 108 Stat. 4279 (October 5, 1994) (codified at 47 USC §§ 1001-1010).
[16] Federal Bureau of Investigation, Situational Information Report, Cyber Activity Alert, "Going Dark: Law Enforcement Problems in Lawful Surveillance," June 29, 2011, http://info.publicintelligence.net/FBI-GoingDark.pdf.
[17] State and local government agencies have also issued reports and statements on the debate. *See*, *e.g.*, "Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety," November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.
[18] James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[19] Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, "Encryption and Cyber Security for Mobile Electronic Communication Devices," Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, April 29, 2015, http://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.
[20] Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, "Encryption and Cyber Security for Mobile Electronic Communication Devices," Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, April 29, 2015.
[21] James B. Comey, "Counter Intelligence and the Challenges of Going Dark," Statement Before the Senate Select Committee on Intelligence, July 8, 2015, https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark; https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy; James Comey, "Encryption, Public Safety, and 'Going Dark,'" *Lawfare*, July 6, 2015, https://www.lawfareblog.com/encryption-public-safety-and-going-dark. *See also* Michael Steinbach, "ISIL in America: Domestic Terror and Radicalization," Statement Before

the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, February 26, 2015, https://www.fbi.gov/news/testimony/isil-in-america-domestic-terror-and-radicalization.

[22] James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014.

[23] James Comey, Oral Testimony Before the U.S. Senate Committee on the Judiciary, "Oversight of the Federal Bureau of Investigation," December 9, 2015.

[24] John Reed, "Transcript: NSA Director Mike Rogers vs Yahoo! on Encryption Backdoors," Just Security, February 23, 2015, http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/; Nick Gass, "Jeh Johnson warns of post-Snowden encryption frenzy," *Politico*, May 15, 2015, http://www.politico.com/story/2015/05/jeh-johnson-edward-snowden-fallout-117986.html.

[25] *See* Damian Paletta, "Paris Attack Reopens U.S. Privacy vs Security Debate," *The Wall Street Journal*, November 16, 2015, http://blogs.wsj.com/washwire/2015/11/16/paris-attack-reopens-u-s-privacy-vs-security-debate/.

[26] Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear of ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

[27] James B. Comey, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption," Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

[28] Ellen Nakashima and Andrea Peterson, "Obama administration opts not to force firms to decrypt data – for now," *The Washington Post*, October 8, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[29] Cyrus Vance, Fraçois Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *The New York Times*, August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

[30] *See* Rowena Mason, "U.K. spy agencies need more powers, says Cameron," *The Guardian*, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks; Rob Price, "The U.K. government insists it's not going to try and ban encryption," *Business Insider*, July 14, 2015, http://www.businessinsider.com/uk-government-not-going-to-ban-encryption-2015-7.

[31] *See* David Sanger and Nicole Perlroth, "Encrypted Messaging Apps May Face New Scrutiny Over Possible Role in Paris Attacks," *The New York Times*, November 16, 2015, http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html.

[32] *See* Paul Mozur, "New Rules in China Upset Western Tech Companies," *The New York Times*, January 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-

companies.html; Zack Whittaker, "E.U wants to force Internet, phone companies to turn over encryption keys," *ZDNet*, January 22, 2015, http://www.zdnet.com/article/eu-wants-internet-phone-companies-to-hand-over-encryption-keys/; Paul Hockenos, "Europe Considers Surveillance Expansion After Deadly Attacks," *The Intercept*, January 20, 2015, https://firstlook.org/theintercept/2015/01/20/europe-considers-surveillance-expansion/.

[33] To give but a few examples, *see* Hal Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol.1(1) (2015); Kenneth Dam and Herbert Lin, eds., *Cryptography's Role in Securing the Information Society* (National Academies Press: Washington, DC, 1996); Hal Abelson, Ross Anderson, et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," (1997); Peter Swire and Kenesa Ahmad, "Encryption and Globalization," 13 *Columbia Science & Technology Review* 416 (September 2012); Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st" in Karl De Leeuw and Jan Bergstra (eds.), *The History of Information Security* (Elsevier, 2007). Technology companies have also joined members of civil society, academics, and security technologists in recent public statements concerning the debate. *See* Kevin Bankston, "Massive Coalition of Security Experts, Tech Companies and Privacy Advocates Presses Obama to Oppose Surveillance Backdoors," New America Foundation, Open Technology Institute, May 19, 2015, https://www.newamerica.org/oti/massive-coalition-of-security-experts-tech-companies-and-privacy-advocates-presses-obama-to-oppose-surveillance-backdoors/.

[34] Hal Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Vol. 1(1) (2015).

[35] *Maximillian Schrems v. Data Protection Commissioner*, C-362/14 (CJEU October 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[36] David Kaye, Human Rights Council, United Nations, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," May 22, 2015. *See also* David Kravets, "U.N. says encryption 'necessary for the exercise of the right to freedom'," *Ars Technica*, May 28, 2015, http://arstechnica.com/tech-policy/2015/05/un-says-encryption-necessary-for-the-exercise-of-the-right-to-freedom/.

[37] *See* Peter Swire and Kenesa Ahmad, "'Going Dark' Versus a Golden Age of Surveillance," Center for Democracy & Technology, November 28, 2011.

[38] Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," *MIT Technology Review*, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.

[39] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," 12 *Northwestern Journal of Technology and Intellectual Property* 1 (April 2014).

[40] *See*, *e.g.*, Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World," *MIT Technology Review*, November 24, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-

can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.

[41] *See*, *e.g.*, Google, "Showing Gmail ads," https://support.google.com/adwords/answer/6105478.

[42] Facebook, "How to target Facebook Ads," https://www.facebook.com/business/a/online-sales/ad-targeting-details.

[43] Yahoo, "Advertising," https://advertising.yahoo.com/.

[44] Michael Ambrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[45] *See*, *e.g.*, Dropbox, http://dropbox.com/.

[46] *See*, *e.g.*, Janna Anderson and Lee Rainie, "The future of cloud computing," Pew Research Center, June 11, 2010, http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/.

[47] *See* Quentin Hardy, "The Era of Cloud Computing," *The New York Times*, June 11, 2014, http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/.

[48] Apple, "iOS Security," September 2015, https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[49] Nicholas Weaver, "iPhones, the FBI, and Going Dark," *Lawfare*, August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.

[50] Zach Miners, "End-to-end encryption needs to be easier for users before Facebook embraces it," *PC World*, March 19, 2014, http://www.pcworld.com/article/2109582/end-to-end-encryption-needs-to-be-easier-for-users-before-facebook-embraces-it.html.

[51] Andrew Cunningham, "Google quietly backs away from encrypting new Lollipop devices by default," *Ars Technica*, March 2, 2015, http://arstechnica.com/gadgets/2015/03/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/; Timothy J. Seppala, "Google won't force Android encryption by default," *Engadget*, March 2, 2015, http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/.

[52] Alex Dobie, "Why you'll never have the latest version of Android," *Android Central*, September 6, 2012, http://www.androidcentral.com/why-you-ll-never-have-latest-version-android.

[53] Android Developer Dashboards, http://developer.android.com/about/dashboards/index.html (visited January 27, 2016).

[54] *See*, *e.g.*, Anton Troianovski, "Phone Firms Sell Data on Customers," *The Wall Street Journal*, May 21, 2013, http://www.wsj.com/articles/SB10001424127887323463704578497153556847658; Julianne Pepitone, "What your wireless carrier knows about you," *CNN Money*, December 16, 2013, http://money.cnn.com/2013/12/16/technology/mobile/wireless-carrier-sell-data/; Declan McCullagh, "Verizon draws fire for monitoring app usage, browsing habits," *CNET*, October 16, 2012, http://www.cnet.com/news/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/.

[55] McKinsey, "Unlocking the Potential of the Internet of things," June 2015. http://www.mckinsey.com/insights/business_technology/The_Internet_of_Things_The_value_of_digitizing_the_physical_world.

[56] *See* McKinsey, "Unlocking the Potential of the Internet of things," June 2015.

[57] *See* Janna Anderson and Lee Rainie, "The Internet of Things Will Thrive by 2025," Pew Research Center, March 14, 2014, http://www.pewinternet.org/2014/05/14/internet-of-things/.

[58] *See* Kelsey Finch and Omer Tene, "Welcome to the Metropicon: Protecting Privacy in a Hyperconnected Town," 41 *Fordham Law Review* 1581 (October 2014).

[59] *See*, *e.g.*, "Discover the internet of things," http://iolist.co.

[60] *See*, *e.g.*, https://aws.amazon.com/iot/; http://www.apple.com/ios/homekit/; https://developers.google.com/brillo/.

[61] *See* David Linthicum, "Thank the cloud for making big data and IoT possible," *InfoWorld*, January 16, 2015, http://www.infoworld.com/article/2867978/cloud-computing/thank-the-cloud-for-making-big-data-and-internet-of-things-possible.html.

[62] *The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003). *See also* Adam Liptak, "Court Leaves the Door Open For Safety System Wiretaps," *The New York Times*, October 21, 2003, http://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html, and Jonathan Zittrain, *The Future of the Internet – And How to Stop It* (2008), "Tethered Appliances, Software as Service, and Perfect Enforcement," http://yupnet.org/zittrain/2008/03/14/chapter-5-tethered-appliances-software-as-service-and-perfect-enforcement/.

[63] There are numerous consumer products – including baby monitors, security cameras, and even children's toys – with networked sensors that rely telemetry and other data to third-party intermediaries for processing and other purposes. *See*, *e.g.*, "Amazon Echo," http://www.amazon.com/gp/product/B00X4WHP5E/; Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/; Phillips, "In.Sight Wireless HD Baby Monitor," http://www.usa.philips.com/c-p/B120_37/in.sight-wireless-hd-baby-monitor.

[64] *See* Shane Harris, "Your Samsung SmartTV Is Spying on You, Basically," *The Daily Beast*, February 5, 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

[65] Samsung, "Samsung Privacy Policy – SmartTV Supplement," http://www.samsung.com/sg/info/privacy/smarttv.html (accessed October 26, 2015).

[66] Samuel Gibbs, "Google eavesdropping tool installed on computers without permission," *The Guardian*, June 23, 2015, http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.

[67] Ariella Brown, "Smart Barbie Puts Child's Play in the Cloud," *Information Week*, April 5, 2015, http://www.informationweek.com/cloud/smart-barbie-puts-childs-play-in-the-cloud/a/d-id/1319779.

[68] Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/.