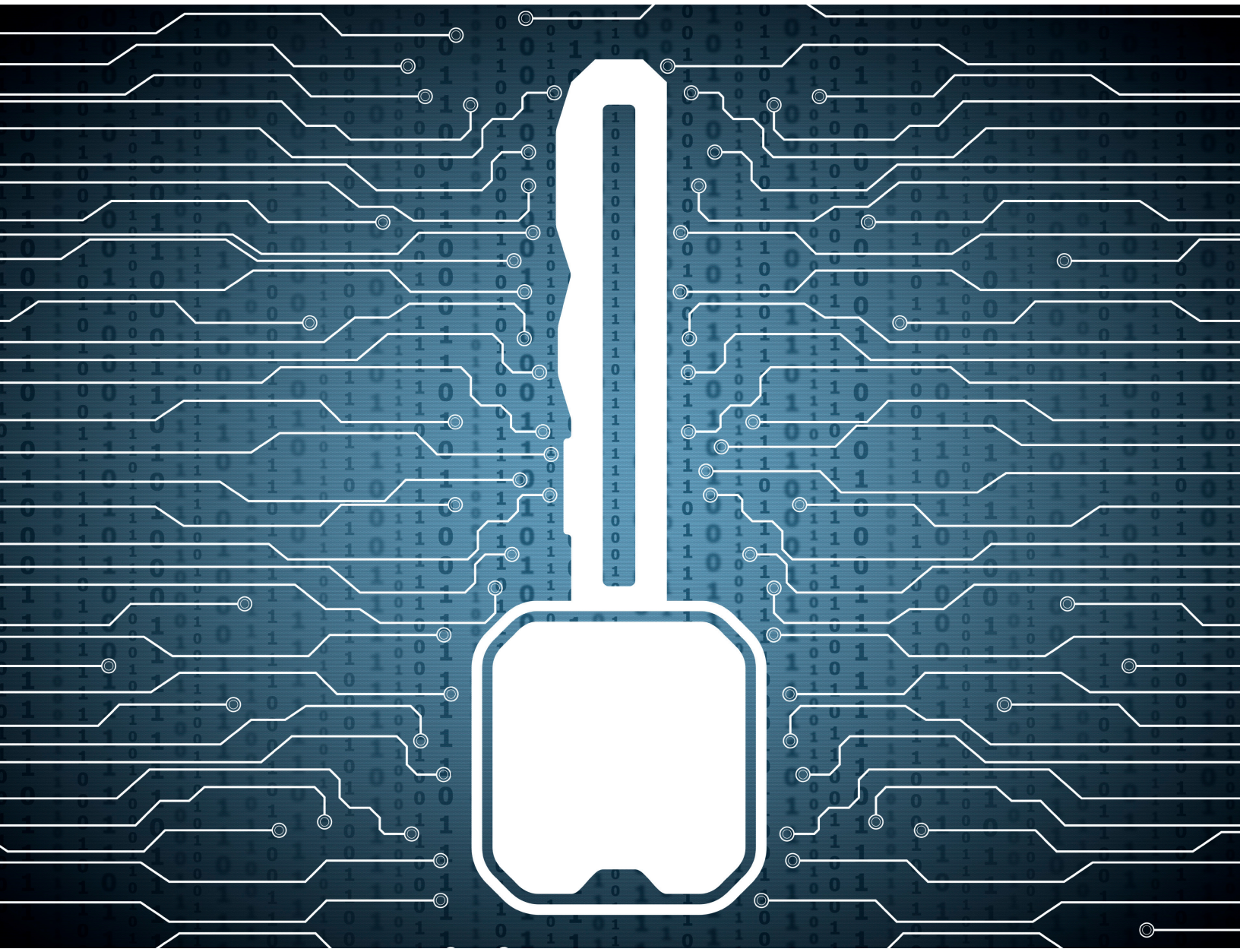
WHITE PAPER

The Ground Truth About Encryption

And The Consequences of Extraordinary Access



THE CHERTOFF GROUP

Abstract: U.S. policy makers are currently engaged in a debate regarding the merits of mandating a means of "extraordinary access" to encrypted data for U.S. law enforcement, what is sometimes referred to as an encryption "backdoor." This paper examines modern encryption technologies, the feasibility of providing law enforcement with extraordinary access, the impact that encryption technology is currently having on U.S. law enforcement (which some have referred to as "going dark"), and the likely impacts that an extraordinary access requirement would have on U.S. national security, the technology sector, and continued innovation in the security field. We conclude that an extraordinary access requirement is likely to have a negative impact on technological development, the United States' international standing, and the competitiveness of the U.S. economy and will have adverse long-term effects on the security, privacy, and civil liberties of citizens.

Introduction

We are in the midst of a significant legal, technical, and policy debate in America (and around the globe). The question is whether governments may lawfully access digital communications and digitally stored data. The question manifests itself in many ways, ranging from the extraterritoriality of legal process to requirements for data localization.

One of the most prominent aspects of the debate pertains to the changing nature of how users and service providers encrypt data. For our purposes, we use the word "encryption" to mean the encoding of data or information in a way that is intended to prevent access to that data or information by persons or parties whose access is not authorized by the creator of the data.

The outlines of the issue are clear. For years, most users kept their data on their own local devices (smart phone, tablet, laptop, etc.) in an unencrypted form. Others backed up their data using cloud storage service providers – providing the user with easy access but, also allowing the cloud storage provider to access the data, both purposefully (for business reasons) and, as more relevant to our discussion, under compulsion of law. Most users sent messages to friends and colleagues in unencrypted or readily decryptable formats. As a result, under the status quo of five years ago, a government could readily achieve lawful access (that is, purposeful requests to access data as part of an investigation, made by law enforcement and subject to a judicial or administrative authorization process, according to an established rule of law) to unencrypted data related to its inquiry – by accessing the data on the user's local device, by accessing it in cloud storage, or by intercepting the unencrypted communication while in transit.

Two developments in the last year or two are rapidly changing that reality:

- First, device manufacturers are adopting operational systems that have changed the default local encryption setting from "off" to "on." In other words, data on local devices was previously stored in an unencrypted form unless the user manually chose to enable the encryption option, but now the converse will be true – affirmative action by the user is necessary to store data in an unencrypted form.
- Second, service providers are taking steps to offer users products that automatically encrypt data stored in cloud storage systems and messages transmitted to other people in a manner that cannot be decrypted by the service providers. Put another way, service providers are offering products that prevent them from being technically capable of responding to lawful government demands as they cannot turn over data they do not possess.

To some degree, these changes are a natural technological evolution. They are also a response to pervasive concerns about the insecurity of cyber systems and to the business necessity of distinguishing commercial products from governmental activity. Whatever the reason, the upshot of these two trends is of growing concern for law enforcement and other government agencies that are systematically losing access to data and information relevant to criminal, national security, and counter-terrorism efforts. As a consequence, some in the community, most notably the Director of the Federal Bureau of Investigations (FBI)[1], have called for new laws or policies that restrain, limit, or even reverse the underlying technological trends.

This white paper, produced by The Chertoff Group, reflects our collective understanding of the issues and challenges posed by the growth in the availability and ubiquity of encryption technology. Our intention is to provide in a single place a readily understandable, comprehensive assessment of the issue.

This white paper, produced by The Chertoff Group, reflects our collective understanding of the issues and challenges posed by growth in the availability and ubiquity of encryption technology. Our intention is to provide a readily understandable, comprehensive assessment of the issue. We want to ask both descriptive questions about the availability of encryption technology and their effect on law enforcement, as well as normative ones about the proper balance between security and liberty. We hope to shed light on a discussion that is often cloaked in the darkness of technical jargon and national security classification so that debate on the topic can be based on a common, baseline understanding of the law, policy, and technology of encryption.

This white paper is comprised of the following parts:

- We begin with a primer on encryption technology, explaining the history of encryption techniques, how they work, and why they are more powerful today than they were a generation ago;
- We then situate this technological development in the context of today's debate about lawful access (sometimes called "extraordinary access" or a "backdoor" requirement) to encrypted data;
- We then examine the ground truth about encryption today. Based on available, open source information, we conclude that:
  - The spread of strong consumer encryption technology around the globe is inevitable;
  - Encryption technology has, to date, been an impediment to successful law enforcement, but the magnitude of that impediment is modest;
  - We can find no successful terrorist attack that would have been prevented by the availability of a lawful decryption access technology, but in the future it is likely that ubiquitous encryption will have an impact on law enforcement capabilities;
  - Requiring exceptional access is unlikely to be as productive as law enforcement hopes it will be – especially when it comes to determined, motivated, and technologically-savvy actors, some of whom have already begun to abandon the usage of American communication platforms; and
  - Engineering an exceptional access capability into existing encryption systems is a massively complex technical undertaking, and the more complex a system is, the less secure it is.
- Finally, we look at some of the anticipated consequences that might arise from mandating lawful access to encrypted data for American encryption products.
  - We should not overstate the practical significance of any decision the U.S. might make. It is uncertain that authoritarian nations (e.g. China or Russia) will forgo implementing an encryption access requirement simply because the U.S. chooses not to (or vice versa);
  - It is possible (and perhaps even highly likely) that mandating exceptional encryption access would hinder or damage innovation in the U.S. encryption technology market. It may also restrain innovation in related U.S. security technology markets;
  - Adoption of an American encryption access requirement may result in adverse collateral effects, decreasing law enforcement's investigative access to metadata and hampering the competitiveness of American businesses and U.S. national security; and
  - Efforts to constrain encryption through forms of extraordinary access will inevitably introduce vulnerabilities into the security of consumer products in ways that are likely to have adverse long-term effects on the security, privacy, and civil liberties of citizens.

In the end, this analysis leads us to the firm conclusion that the effort to mandate an extraordinary access requirement is problematic at best, and at worst may appreciably degrade national security – most directly, the security and privacy of U.S. businesses and citizens – and diminish American economic competitiveness, international standing, and technological capabilities. Thus, we would not recommend adoption of such a proposal and we urge Congress and the Executive Branch to exercise extreme caution as they consider the issue.

Understanding Encryption

Sound public policy on technology rests on solid technical foundations.[2] Because many policy makers confronted with difficult encryption policy questions may not understand the technical details, we begin by offering this brief summary of encryption technology.

> Encryption, or secret writing, is one of the oldest forms of human activity.

Encryption, or secret writing, is one of the oldest forms of human activity. Secret coding has existed for as long as there have been secrets worth keeping. But there is a difference between hiding a message and encoding a message. Hiding merely provides a means of preventing the message from being intercepted and detected while en-route. Encryption, or encoding, is intended to keep the message secret even if it is physically intercepted.

Private Keys

The oldest form of encryption is based on private keys, or encryption keys shared privately between two parties. Conceptually, private key encryption involves three separate components that come together – the "plaintext," the "algorithm," and the "key." The "plaintext" is the substance of the message that the sender wants to convey. This information may not be "text" at all; it can be the firing code for a nuclear missile, the formula for Coca Cola products, or any data of any form that is more valuable to the sender if it is not known to anyone other than the intended recipient.

The "algorithm" is a general system of encryption, or a general set of rules for transforming a plaintext. An example of an algorithm is a cipher in which each letter of the plaintext (assuming it is actually a written text) is replaced with another letter. The algorithm here is "replace each letter with another."

The third and most vital component of an encryption system is the "key," or the specific set of instructions used to apply the algorithm to a particular message. A cipher key might therefore be "replace the letter with the letter five letters after it in the English alphabet." Using this simple algorithm and key, the plaintext "cat" would then be converted to the word "hfy" and that result would now be known as the "ciphertext." The critical feature is that, as an initial premise, only someone with the algorithm and the key can decrypt the ciphertext, protecting the content even if it is physically intercepted.

We've been creating ciphertext for quite a long time. Earliest mentions of coded writing can be found in the *Kama Sutra*, which counseled women to record their liaisons in secret writing. Julius Caesar's use of codes was so common that his preferred algorithm, the letter shift system mentioned above, is sometimes called the Caesar cipher.[3]

Naturally, where some seek to keep secrets, others seek to reveal them. It is one of the truisms of encryption that the "key" to keeping a secret is the key, not the algorithm. The algorithm – the general method – is often too widely known to be usefully kept secret. So the strength of the key – how difficult it is to guess – defines the strength of the encryption product.

To return to the Caesar cipher, if we restrict ourselves to just shifting the alphabet, there are only 25 possible keys to use, depending on how far down the alphabet we shift the letters. That's a pretty weak key – if someone knows the general algorithm, then the key can be cracked in a short time period through repetitive testing of possible solutions—trial and error. This method is commonly described as "brute force." If we loosen the algorithm a bit, and instead of a "shift" rule we apply a rule that allows any rearrangement of the 26 letters of the English alphabet, then the number of keys increases astronomically to well over 400 septillion different possible arrangements, making a brute force effort to discover the key more difficult. Thus, private key encryption is effective if (and only if) the decryption key is kept private – hence its name.

Frequency Analysis

Of course, brute force is not the only method of breaking a cipher. Since at least the 9th century (when the method of frequency analysis was first reported by Arab scholars)[4], scholars have demonstrated that a cipher can be broken by analysis rather than brute force. Frequency analysis is relatively simple – it rests on knowledge that is external to the code itself. For example, in English the letter "e" is the most common vowel. Other common letters in regular usage include "a," "i," "n," "o," and "t." With this knowledge about the English language, the deciphering of a ciphertext is made much easier. It is very likely that the most frequently used cipher letter, whatever it may be, represents one of these common English letters. In a ciphertext of any reasonable length, there is virtually no chance, for example, that the most common cipher letter is being used to signify a "q" or a "z."

To defeat such frequency analysis, cryptographers used sophisticated key systems that seemed to change over time. A notable example is the Nazi Enigma code, which was thought to be functionally unbreakable because it seemed on the surface not to follow a one-to-one

mapping between ciphertext and plaintext. So if the encryptor wanted to encode the letter "b," sometimes the key would use an "r," sometimes an "i," sometimes a "q," and so on. Conversely, no character within the cipher automatically denoted a single character in the plaintext, so the rule appeared unspecified in both directions.

This was actually a superficial complexity made possible by circuitry within the Enigma machine. At the start of every transmission, the German officer would explicitly need to state certain settings (the key) that the receiver would then program into his own Enigma device in order to make sense of the message. So the Enigma code was essentially no more sophisticated than the Caesar shift rule, though certainly more complex and labor-intensive.

In the end, knowledge of frequency analysis makes decryption easier and reduces the need for utilizing a brute force approach. It is a fair assessment of the art of cryptography that, until the dawn of the computer era, those decrypting ciphers had the upper hand. Either the keys themselves could be stolen, or they could be decrypted using sophisticated techniques like frequency analysis.

The Prime Number, Public Key Revolution

There things stood for a number of years. Those who wanted to keep secrets were at a fundamental disadvantage – in order to transmit a secret message, they first had to exchange a secret key to the message.[5] Besides the possibilities of backward analysis to determine the key, a multitude of problems with the exchange of keys existed. They could be lost, stolen, revealed, or compromised in any number of ways. By their very nature, private keys, whose encryption and decryption algorithm were known only to the sender and the recipient, were only good as long as they were private.

In the late 1970s, enterprising cryptographers developed a way to encrypt information using the multiplication of two impossibly large prime numbers and certain one-way mathematical functions (a one-way function is one that only works in one direction; most mathematical functions, like addition and subtraction, work in both directions – you can get the results from the precursors or the precursors from the results). With one way functions, a recipient is able to publish the result of his impossibly large multiplication as a public key, while retaining the decryption key as a private key. To work, he is no longer required to share his private key with the sender. Instead, people who wanted to send the recipient a message could use the public key to encrypt their message. And since only the recipient knew how to break down his impossibly large number to its original primes – because he has the only corresponding private key – only he could decrypt the message.[5] Today, you can embed this type of encryption into your e-mail system using a program that can be purchased over the Internet for less than $100. If the users at both ends of a message use this form of public key encryption, the secret message they exchange between themselves becomes, effectively, undecryptable by anyone other than the key's creator,[6] unless, of course, a hacker attacks the creation of the key at its source by breaking into the key generation algorithm or stealing the decryption key from the key's creator.

> In short – and this is the single most important policy takeaway – properly implemented public key encryption is essentially undecryptable. And so, the legal and policy questions focus on who holds the decryption key and can they be compelled by law to turn it over to the government under certain defined circumstances?

In short – and this is the single most important policy takeaway – properly implemented public key encryption is essentially undecryptable.[7] And so, the legal and policy questions focus on who holds the decryption key and can they be compelled by law to turn it over to the government under certain defined circumstances?

End Point, In-Transit, and Service Provider Encryption

One final distinction must be drawn to complete this outline of the basics of encryption – an important difference between endpoint encryption; end-to-end or "in-transit" encryption; and service provider encryption.[8] This is a common technological distinction and one with critical legal ramifications.

Service-provider encryption

> If a cloud provider encrypts the data for the user, then the provider holds the encryption key and the relevant legal and policy question is when (if ever) that provider can be obliged to turn over that key to a third party.

Google, Microsoft, Dropbox, Apple, and other cloud service providers have, in the past, used forms of service-provider encryption. When one stores data in Dropbox or leaves e-mail in a Gmail folder on the web, that data is encrypted by the service provider. Their encryption techniques are, generically, quite strong – and that makes them relatively well-protected against outside attack by malevolent actors. But the reality is that for this form of long-term storage, the service provider itself retains the encryption key. That's the functionality

that, in the end, allows a user to log in to Microsoft or Box from several different machines. The username and password combination – increasingly paired with a second factor of authentication – enables the decryption of the contents in cloud storage. This is the type of encryption that almost all conventional users enable – it's quick, effective, and seamlessly integrated into your application. But if a cloud provider encrypts the data for the user, then the provider holds the encryption key and the relevant legal and policy question is when (if ever) that provider can be obliged to turn over that key to a third party.

Endpoint encryption

By contrast, with endpoint encryption, the user holds the encryption key. For example, if one uses a strong encryption program locally on the user's own hard drive and then uploads the encrypted file to a cloud storage location, the fact that the cloud provider further encrypts the data is good but irrelevant in respect to outside access to the data. Even if the provider were compelled by a lawful order to give the government its decryption key, all that it could turn over is the encrypted file – which would still be encrypted gibberish to the government. Likewise, files that are encrypted and stored locally on a laptop or external hard drive are under the exclusive control of the user who encrypts the data. Indeed, as we discuss further below, this is precisely what some tech companies, like Apple and Google, are doing – making this on-device encryption the default setting.

End-to-end encryption

Finally, consider end-to-end encryption, or the encryption of messages that are in transit from a sender to a receiver. This form of encryption, sometimes called gateway encryption, is not nearly as easy to do, not as widely available, and not as seamlessly integrated as endpoint encryption. For example, even though some users have installed PGP, a privacy encryption program that one can use for e-mail exchanges, it is ineffective unless the recipient also has the same program. If they both have it, the program acts as endpoint encryption such that the message would be nearly impossible to read even if the National Security Agency (NSA) were to intercept it. But few people, until now, have used PGP or its modern equivalents. It isn't seamlessly integrated into e-mail programs and so it falls by the wayside. That technological reality is changing, as businesses develop new, more user-friendly end-to-end encryption programs. For now, however, the penetration of those programs into the general consumer market remains limited.

So that's the architectural issue. Sometimes the user holds the encryption keys and sometimes the service provider – Google, etc. – does. Who does makes a world of legal difference.

Technical Options for Exceptional Access

When it comes to exceptional access, a number of different ideas have been proposed. While each is different, all generally fit into one of three basic approaches:

1. Weaken encryption systems (either by weakening algorithms or systems that support key distribution) – this allows law enforcement or other parties to more easily circumvent encryption and read communications.
2. Create a "golden key" – enabling the holder of that key to bypass other encryption controls and read communications.
3. Require that all users securely escrow their encryption keys – giving law enforcement or other parties the ability to access someone's keys and use it to read their communications.

The first option is most readily dismissed – it is a ground truth that the use of weaker encryption systems creates a vulnerability that would be used by government and adversaries alike. When you create a backdoor for law enforcement or intelligence agencies you are creating a vulnerability that "may also end up being used for nefarious ends by rogue spooks, enemy governments, or malefactors who wish to spy on the law-abiding."[9]

The second option is functionally equivalent to the first; if a master key enabling access through a "back door" exists, it represents another entry point into a system and serves as a functional equivalent of weakening the algorithm.

An approach relying upon escrowing duplicate keys might initially appear to have some advantages. First, relying on a duplicate key does not, in and of itself, weaken the underlying encryption algorithm. Second, keys that are securely escrowed and accessible only in the event that a warrant was issued could, in theory, address some of the concerns about misuse of this capability.

> Given how cryptographic systems are constructed today, there is no way to escrow an encryption key without increasing the attack surface of the underlying encryption system by several orders of magnitude.

The primary issue here is the word "securely." Given how cryptographic systems are constructed today, there is no way to escrow an encryption key without increasing the attack surface of the underlying encryption system by several orders of magnitude.

In theory, it is technically feasible to construct a key escrow system. But such a system would introduce so many new potential points of attack that it would significantly decrease the overall level of security. Moreover, it would require today's encryption tools – including most PCs, laptops, and mobile devices – to be completely reengineered.

The reason lies in how modern-day asymmetric cryptographic solutions are constructed. Best practices for secure devices dictate that cryptographic keys are often generated in specialized hardware devices that protect each key; examples of these "cryptomodule" solutions include Hardware Security Modules (HSM), Trusted Platform Modules (TPM) chips, Secure Elements and Trusted Execution Environments (TEE).[10] These cryptomodules are specifically designed to ensure that the private keys they generate never leave the cryptomodule; the sensitivity of these keys is believed to be so important that any path allowing the keys to be exported from the cryptomodule would erode the security model of the system.

Indeed, the Federal government mandates that when it comes to the cryptographic keys on the Personal Identity Verification (PIV) smart cards – used by all employees to authenticate into Federal systems – "*the PIV Card shall not permit exportation*."[11] To do so would undermine the broader security model of the PIV Card, creating opportunities to tamper with the keys or otherwise compromise the security of the system.

This non-exportable approach is not unique to government; it is a best practice followed by many other cryptographic security systems today.

Against that backdrop: when we discuss "key escrow" schemes, what we really mean is that we would move from a model in which keys that are generated in secure cryptographic devices can never leave those devices, to one in which we must:

1. Find a safe way to export a copy of each key from each device only for key escrow purposes, but never for any other purposes.
2. Then, find a way to safely transport the key to the key escrow location, without the key being intercepted or compromised.
3. Then, find a way to securely store that key alongside millions – or potentially billions – of other keys, without compromising any keys.
4. Finally, find a way to then manage access to those keys and ensure that someone in the entity trusted to escrow the keys does not compromise them.

Every one of these steps creates multiple opportunities for an adversary to attack and compromise the security model of the underling cryptographic system. Individually, each of the four steps creates a significant security challenge; requiring all four steps creates a multitude of complexities that expands the "attack surface" of the cryptographic system.[12]

In simpler terms: while it may be theoretically feasible to construct a key escrow system, in practice, doing so would create a cluster of new risks.

In simpler terms: while it may be theoretically feasible to construct a key escrow system, in practice, doing so would create a cluster of new risks. A ground truth in computer security is that risk can be measured by using the simple equation: *Risk = Threat x Vulnerability x Consequence*. While we do not delve into a line-by-line scoring of the risks presented by key escrow in this paper, it is clear that each of the four tasks above create material threats and vulnerabilities, each with significant consequences relative to today's best practices for creating keys with cryptomodules.

Given how much industry has struggled to securely implement even simple cryptographic systems, it is our judgement that a solution this complicated would be certain to create significant risks and degrade our overall security.

Given how much industry has struggled to securely implement even simple cryptographic systems, it is our judgement that a solution this complicated would be certain to create significant risks and degrade our overall security.

Beyond the technical and security challenges, the practical impact of this would be to break current best practices for secure key generation and storage. Most cryptographic systems used today would require redesign; given that these systems are embedded in most desktops, laptops, and mobile devices, the software used to manage cryptographic systems in billions of devices would have to be re-engineered, and in some cases the devices themselves would have to be replaced. In theory, this would be technically feasible; in practice, we believe it is highly unrealistic.

Where We Are Today – The Default Debate

These varied methods of encryption – as well as the technical and security ground truths involved with changing the way the technology works – explain the current landscape of policy conflict surrounding encryption. As we have noted, well implemented encryption provides significant security gains to users. And the technology and service provider business models are morphing such that encryption technology has become more readily available to the average consumer, covering both data in cloud storage and encrypted local storage. Google made Secure HTTP (HTTPS) the default for its Gmail service in 2010 and for Google web searches in 2011. This effectively strengthened encryption and reduced the ability of hackers to mine historical communication data by implementing an encryption concept called "forward secrecy," which we discuss later in this paper.[13] This trend continues today: Google is planning to introduce additional forms of encryption into its services, Yahoo has added support for end-to-end encryption to e-mail services, and Apple supports default end-to-end encryption for iMessage.[14] Law enforcement and counter-terrorism efforts will, inevitably, be affected by these changes in the data landscape – an effect whose magnitude and scope have yet to be determined.

> In our judgment, the dispute about the availability of strong or perfect encryption is not new – the technology has been both legal and widely available for years.

In our judgment, the dispute about the availability of strong or perfect encryption is not new – the technology has been both legal and widely available for years. That debate was first raised and resolved more than 15 years ago at the time of the Clipper Chip proposal.[15] Rather, the question of encryption is brought to a head by technology companies' decisions to change default hardware and software settings from a model in which mass-market communication systems and storage devices come with encryption set to a default "off" setting to one where the default setting is "on."

We do not doubt the significance of this change. The concept of default bias in behavioral science is well known. It is why many privacy advocates favor privacy by default, recognizing the importance of default settings to final outcomes.[16] For much the same reason, technology companies fight to be designated as the default browser or e-mail system in a new software package.[17] The basic answer is clear: default settings win – they are what consumers use, even when they have the capacity to make changes.[18]

Default bias is particularly powerful in the software and internet settings in which encryption is at issue.[19] Most users are relatively technology illiterate, and that is true even among users who are privacy-sensitive. In one study of user privacy settings, research revealed that a random collection of users couldn't even successfully adjust their default privacy settings – making the default even more prominent.[20]

Whether the strong encryption function comes as a default option or as an option you can choose is likely to matter a great deal, at least to the overwhelming majority of mass market users. Ironically, it may have significantly less effect on sophisticated users – including criminals – who are aware of the possibility, capable of managing their own encryption experience, and have the incentive to bear the transaction costs and do so successfully.

> The best way to protect the security and privacy of consumers is by making the "on" option for strong encryption the default one.

The recent series of steps by technology companies to enable default strong encryption is a response to this default bias, and to the increasingly sophisticated nature of cyberattacks against consumers and their products. As several technology companies put it recently, in response to a UK lawful access proposal: "User trust is essential to our ability to continue to innovate and offer our customers products and services, which empower them to achieve more in their personal and professional lives."[21] Put another way, the best way to protect the security and privacy of consumers is by making the "on" option for strong encryption the default one.

Ground Truth – How Damaging to Law Enforcement is Encryption?

While many suggest that encryption could have crippling effects on law enforcement and counter-terrorism efforts, is that true? What is the record, to date, with respect to how encryption has (and has not) produced adverse consequences on lawful government activities?[22]

Our assessment is simple – there is very little concrete data (as opposed to anecdote) that bears on the question. What little data there is suggests that encryption technology has, in fact, been an impediment to successful law enforcement but that the magnitude of that impediment is modest. This state of affairs is not necessarily likely to persist – ubiquitous encryption will have a negative impact on law enforcement capabilities. The magnitude of that impact is, however, at this time indeterminate.

The Limited Statistical Data

One of the few neutral sources that reports on the direct impact of encryption on law enforcement investigations is the annual U.S. Courts Reports on Federal and State Wiretaps. Issued each year at the direction of Congress, the reports provide insight into the number, type, location, and duration of Federal and State wiretaps in a given calendar year.

Based on these reports, there is a very modest reported impact from the use of encryption technology. In 2014, the latest year for which a report is available, Federal and State judges authorized 3,554 wiretaps in the U.S., a decrease of 1% from 2013. Of the wiretaps issued in 2014, 96% were issued for portable devices, such as smartphones. Despite the large number of wiretaps authorized for mobile devices, law enforcement only encountered some form of encryption in 22 of the wiretaps, a decrease of 46% from 2013. In only two of those cases were law enforcement unable to decipher the plain text of the messages.[23] Likewise, in 2013, the police reported nine cases in which law enforcement could not decrypt an intercepted communication.[24]

Still other data has been provided by Cyrus Vance, the Manhattan District Attorney. Mr. Vance testified before the Senate Judiciary Committee regarding encryption and public safety on July 8, 2015. Vance identified a number of serious crimes in which data obtained from a suspect's mobile device was particularly important to the investigation. In his testimony, Vance tallied 74 Manhattan cases from July 2014 to July 2015, in which a law enforcement investigation was "hindered" as a result of law enforcement's inability to access device data due to device encryption.[25] The Manhattan District Attorney's Office later updated this figure to 111 to cover the year October 2014-October 2015.[26] What "hindered" means is unclear.

> In other words, encryption hindered an investigation in roughly one tenth of one percent of the cases handled by the Manhattan DA's office.

For context, it is useful to note that the figures cited by the Manhattan District Attorney's office are a small percentage of the more than 100,000 criminal cases that the office handles each year. In other words, encryption hindered an investigation in roughly one tenth of one percent of the cases handled by the Manhattan DA's office.[27] While these statistics represent just one local U.S. jurisdiction, these are the only statistics that have been released and cited by the law enforcement community on this issue. Of course, each individual case is important – both to its victims and to the prosecuting authorities. But it remains useful to assess the current scope of the encryption challenge at a systematic level.

Three Recent Incidents – Paris, San Bernardino, CA and Garland, TX

With a limited statistical data set, it is useful to try to assess the utility of encryption as a tool of criminals and terrorists by other means. The most notable alternate methodology is a case study method, using a specific fact-pattern (or set of fact-patterns) to generalize. For that reason we examine three recent incidents of prominence to assess the role of encryption in their execution – the terrorist attacks in Paris, San Bernardino, CA and Garland, TX.[28]

According to some public reports, government officials with knowledge of the Paris attacks have stated that the attackers likely used encrypted messaging applications – specifically WhatsApp and Telegram – to coordinate and plot the attacks.[29] As should be evident, this suggestion of a possible path dependency on encryption technology is not a conclusive attribution. Rather, all we know with certainty at this time is that end-to-end encrypted applications were downloaded on the phones of the Paris terrorists.[30] We also know that on the day of the attack, one of the attackers used SMS messaging on an unencrypted, unlocked phone to communicate plans to the terrorist cell.[31]

As of now, there is no clear evidence that the attackers in San Bernardino, CA used encryption to plan the attack or communicate with a third-party enabler of the plot. News outlets have reported statements made by senior U.S. law enforcement officials that the terrorist couple who conducted the attack possessed devices with "level(s) of built-in encryption,"[32] a reference, we infer, to the standard built-in encryption system

currently available on many devices. On the other hand, investigators have (as of the writing of this paper) not been able to verify whether the couple used encryption to communicate secretly because its technicians have "been unable to get into certain parts of the devices' memory"[33] – an indication, perhaps, of the use of endpoint encryption on some devices.[34]

Finally, one of the two gunmen killed by police on May 3, 2015 while attempting to carry out a terrorist attack on an event featuring cartoons of the Prophet Muhammad in Garland, Texas, exchanged 109 encrypted messages with a known overseas terrorist on the day of the attack. As FBI Director James Comey testified to the Senate Judiciary Committee on December 9, 2015, "we still have no idea what he said because those messages were encrypted."[35] Because law enforcement authorities have not suggested that they were aware of the messages before the shooting, it would be counter-factual to speculate on whether the interception of these messages in an unencrypted state would have prevented the attacks. It is, however, fair and accurate to say that the investigation into the motivations of the attackers and the degree of their connection to overseas terrorists has been hindered by encryption.

Ground Truth – Alternate Investigative Means

> Good investigative practice relies on the concatenation of small, seemingly disparate, pieces of information.

Good investigative practice relies on the concatenation of small, seemingly disparate, pieces of information. Sound analysis is often derived from deductive reasoning. In other words, we don't always have hard facts on which to rely. For that reason, it is a mistaken commonplace to (as so many routinely do) suggest that a particular investigative method may be discarded because there are ready alternatives. While that is often the case, it obscures the fact that each independent investigative method often offers unique benefits in terms of the type and nature of information it can provide.

Conversely, however, each investigative method also has its costs. Some methods are deemed out of bounds because they conflict with fundamental ethical norms or binding law. Others are too expensive or too likely to be abused.

Hence, in our judgment, it is useful to examine what we know about whether alternate investigative means are available that would enable law enforcement and intelligence officials to function in the absence of ready access to decrypted information. We ask that question not, as some might, to suggest that decryption can be readily dispensed with, but rather to ask the more nuanced cost-benefit question that we have identified.

For example, some have argued that a closer examination of the Garland, Texas plot suggests that a focus on antecedent unencrypted social media communications would be a more effective investigative method than concern about the use of encrypted communications. For more than three years, the Islamic State (ISIS) has prolifically used Twitter's unencrypted direct messaging function to recruit, solicit donations, plan attacks, and point sympathizers to their more covert channels on platforms such as Telegram.[36] Elton Simpson, one of the two attackers in Texas, had been the subject of multiple FBI terrorism investigations since 2011, and had been actively and openly communicating with foreign terrorists via Twitter.

Approximately one week before the attempted shooting in Garland, SITE Intelligence Group reported (based on open-source intelligence) that Mohamed Abdullahi Hassan, a known American ISIS jihadist in Somalia, called for an attack on the Garland event on Twitter. Simpson retweeted this call and requested that Hasan send him a direct message.[37] The combination of this information with the metadata from the 109 messages referenced by Director Comey suggests that, had law enforcement actively monitored Simpson, they may have gathered the necessary intelligence to predict and prevent the attack without the ability to break messaging encryption.

Indeed, there are several examples of terrorist plots foiled through conventional means. Numerous plots have been identified by FBI undercover agents since 2010. In many cases, the FBI has been tipped off by social media activity.[38] For example, the Via Railway Plot was thwarted by a tip-off from a concerned member of Toronto's Muslim community.[39] The Wichita Airport suspect was placed under FBI surveillance after stating his desire to commit "violent jihad" against the U.S. and downloading multiple documents relating to jihad

and martyrdom.[40] And in late 2015, the FBI arrested more than 10 people with ties to ISIS, identified in part because they were communicating with ISIS using encryption – in other words, by virtue of the encryption footprint and the metadata it left behind.[41] In short, traditional methods of surveillance, meta-data analysis, social media monitoring, and the use of key-logger endpoint attacks[42] will remain available to law enforcement.

One possible solution – that of compelled disclosure of passphrases by the encryptor – seems likely to us to be of limited value to law enforcement, even as to American users subject to American law. There is a growing debate over the extent of Fifth Amendment privilege. In the Federal courts, the latest word is an Eleventh Circuit case *In Re: Grand Jury Subpoena (U.S. v. Doe)*[43], which held that disclosure of the passphrase could not be compelled by grand jury subpoena. Not all courts agree with this conclusion. In early 2015, the Massachusetts Supreme Judicial Court ruled to the contrary. In *Commonwealth v. Gelfgatt*[44], that Court held that disclosing the passphrase disclosed only the capacity to decrypt, which was a "foregone conclusion" and did not implicate any proof of authenticity, control, or knowledge. That seems to us a highly suspect conclusion – but it is evidence that the legal question is not settled in the least.

We note, however, that even if a passphrase is considered within the ambit of the Fifth Amendment protection against self-incrimination, access to encrypted data may still be possible when that data is protected by a biometric rather than a passphrase. In late 2014, one Virginia court held that a suspect "cannot be compelled [by the police] to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."[45] Given the significant movement toward the use of biometrics as means of authentication in smartphones, this rule of law offers yet another possible way in which law enforcement may still be capable of effective investigation, even in the presence of strong encryption.

> As far as the public record reflects, we can find no successful terrorist attack that would have been prevented by the availability of a lawful decryption access technology.

In the end, we are left with the following conclusion: As far as the public record reflects, we can find no successful terrorist attack that would have been prevented by the availability of a lawful decryption access technology. Again, this state of affairs is not necessarily likely to persist – it is early days for mass-market encryption. Widespread adoption of encryption technology is likely to have a negative impact on law enforcement capabilities, but the extent of the this impact is unclear. As noted, we cannot say the same with respect to the private, classified record, of which we are unaware.

Ground Truth – Evading Encryption Access

The converse of alternate investigative means is alternate means of conducting illegal activity. Just as law enforcement would react to the absence of lawful access to encrypted communications by using alternate means of investigation, malicious actors would react to the presence of lawful access by changing their methods of communication to ones that would not be intercepted, or to ones that employed encryption products manufactured without the lawful access component.

Non-Encrypted Technology

To begin, there appear to be a variety of methods by which malicious actors might use alternative technologies to avoid detection by law enforcement. For example, the relatively low-tech channels of communication that exist on gaming consoles like Sony PlayStation and Microsoft XBOX may actually provide terrorists and criminals a more secure means of communication than encrypted messaging platforms.[46]

There is some evidence that terrorists are using in-game messaging voice-chat features and even actual elements of gameplay to communicate. That is likely the reason that U.S. intelligence agents "embedded themselves in online games like World of Warcraft to infiltrate virtual terrorist" communications.[47] Resource constraints make it unlikely that the government has the ability, however, to actively monitor the plethora of channels used by the hundreds of millions owners of each video game console.[48]

There is also evidence that terrorist groups, including ISIS, are using private networks accessible only via TOR browsers, collectively and colloquially referred to as "the dark web," to communicate anonymously online.[48] According to Aamir Lakhani, senior security strategist at Fortinet, "the dark web has become ISIS' number one recruiting platform," and jihadists from across the globe use the dark web to make anonymous

bitcoin donations into ISIS accounts.[50] Finally, terrorists and criminals continue to employ more "old-fashioned" means of evading surveillance, like using anonymous pre-paid "burner" phones (as at least one foiled Times Square bomber did),[51] changing cell phone sim cards (as the Paris attackers did),[52] or even passing written letters back and forth (as Osama Bin Laden was purported to have done).[53] In-person communication, which was the chief method employed by the San Bernardino couple to plan their 2015 massacre, also remains difficult to intercept and surveil.

Alternate Encryption

Perhaps more importantly, a U.S.-ordered encryption access system would not be globally pervasive. Malicious actors would have other options for encrypted communication applications if they chose. By driving actors away from American products and systems we might have the perverse effect of driving internet traffic and technology companies offshore, depriving our analysts of valuable metadata information. Indeed, as FBI Director Comey made clear in remarks last year,[54] no American proposal would preclude determined malicious actors, who are willing to incur the necessary transaction costs, from acquiring strong encryption technology, given the global market and wide array of sources. That acknowledgement emphasizes, at least to us, that the extraordinary access requirement proposal is less about determined malevolent actors (such as dedicated terrorists and sophisticated criminal gangs) and more about maintaining access to the decryptable communications of average (and below average) users – everyday criminals, for example, or, in the context of an authoritarian state, political opponents.

Examples of this effect can be cited. In February, ISIS issued an order banning fighters from using devices equipped with location-tracking software, particularly Apple devices.[55] By May, members were tweeting to throw out Samsung Galaxy smartphones as well. In fact, according to ISIS' own training manual, the five most highly recommended encryption systems (what they consider the "safest") are made by companies outside the United States — such as Switzerland, where ISIS assumes that the U.S. would have limited access.[56]

Last year, ISIS officials began warning against using WhatsApp, the popular messaging app owned by Facebook, for fear it was being monitored. Officials said operatives should use one of several Western encrypted or hard-to-track messaging apps, such as Surespot, Telegram, or Kik.[57] Thus, there is evidence that over the past year, ISIS and Al-Qaeda operatives have evolved and varied their usage of encrypted smartphone communication programs tremendously, moving from WhatsApp to Kik, Wickr, Surespot, then to Telegram.[58] Likewise, Al Qaeda operatives have developed their own encrypted communications platforms – the latest version of the mobile app is called "Mujahedeen Secrets 2."[59]

For these reasons, we think that requiring exceptional access is unlikely to be as productive as law enforcement hopes it will be – at least when it comes to determined and motivated actors.

For these reasons, we think that requiring exceptional access is unlikely to be as productive as law enforcement hopes it will be – at least when it comes to determined and motivated actors. Highly motivated actors, plagued by neither inattentiveness nor transaction cost concerns, will likely migrate to alternate systems, thereby diminishing our access to valuable metadata. If exceptional access is required, the principle effect will be on the average consumer and the small-time criminal gang – with significant impacts in the form of degraded system security. There will be significantly less effect on high-value terrorist and criminal targets.

Ground Truth – Duplicate Keys and Vulnerability

For the reasons previously explained, among the technology and cryptology communities, there seems to be near (but not total) consensus that creating an exceptional access system with encryption accessible to lawful users (e.g. authorized law enforcement or intelligence officials) but not to malevolent actors would be either technically impossible (in the case of golden keys) or so complex to implement (for duplicate keys) that the overall security of communications would appreciably diminish. In other words, any system accessible to law enforcement might also be accessed by more nefarious actors, and that would further degrade the security of the networks (which are already subject to daily cyber-attacks) used by U.S. citizens and enterprises to exchange and store valuable information.

Any new cryptosystem that adds exceptional access into existing encryption architecture will thus be significantly more vulnerable to an unauthorized actor accessing and covertly using the decrypting mechanism than the previous system.

This argument rests not on the mathematics behind encryption, but on two relatively simple premises: that engineering an exceptional access capability into existing encryption systems is a massively complex technical undertaking, and that the more complex a system is, the less secure it is.[60] Any new cryptosystem that adds exceptional access into existing encryption architecture will thus be significantly more vulnerable to an unauthorized actor accessing and covertly using the decrypting mechanism than the previous system.[61]

This conclusion is, manifestly, a predictive judgment. It is based on a reasonable assessment of the technical complexity of the task combined with a practical assessment of human nature. If there is a door, unauthorized persons will try and open it, and they may likely succeed.

As with the question of encryption as a protection for terrorist activity, there is no systematic data to help us answer the question. We proceed, again, using the case-study method, looking at historical evidence (presented below in chronological order) that bears on the question of whether or not lawful government access can be subverted by malevolent actors. Based on historical record, there is, in our judgment, good reason to be cautious about the ability to create access systems that will not be subverted:

Clipper Chip, 1993-1997: In 1993, the U.S. government proposed the adoption of a new standard "key escrow system" for encryption technologies. Essentially, an NSA-designed encryption device, the Clipper Chip, would encrypt data but also retain a copy of the keys necessary for decryption of the data, which would be held "in escrow" by either the government or a neutral third party that could be compelled to provide the keys to government with proper legal authorization. A year after the first set of clipper-chip enabled products went to market, cryptographer Matt Blaze published a methodology for "bypass[ing] the government access feature while still making use of the encryption algorithm," and identified other technical flaws.[62]

Athens Affair, 2004-2005: For 10 months between 2004 and 2005, a still-unknown party wiretapped and listened in on calls to and from the cellphones of 100 senior Greek government officials, including the Prime Minister and the heads of the defense and justice ministries. The perpetrator was able to exploit the intercept features on an Ericsson telephone switch purchased and operated by Vodafone Greece, the country's leading service provider (and provider for those 100 cell phones). An encryption system back door was at the heart of that intercept system. The perpetrator was able to intercept highly confidential and classified calls for over ten months before finally being detected.[63]

RSA Seed Key Breach, 2011: In 2011, hackers (believed to be state-sponsored) breached RSA (the Security division of EMC) and stole SecurID seed keys – "initial keys used to generate other encryption keys for the hardware token used to provide two-factor authentication tokens."[64] SecurID data was subsequently used to attack RSA customer Lockheed Martin.[65] The RSA breach was not caused by any encryption-related vulnerability. But it is included to illustrate the difficulty of managing and securing encryption keys at scale and makes clear that any repository of encryption key material, such as would be required by a key escrow approach, is a significant target of attack.

Freak, 2015: In the early 1990's, the U.S. government began requiring companies to downgrade the encryption for products being shipped overseas from strong RSA-grade encryption to a not-quite-as strong version of "export-grade" encryption.[66] At the time, "export-grade" encryption was still relatively strong, and it was likely that only the U.S. had the computing capability to crack this encryption key. However, the increase in computing power that has occurred over the past 20 years has created an environment where there is now a significant security flaw in older versions of the cryptographic protocols used to encrypt online communications – SSL and TLS.

In March 2015, researchers from the French Institute for Research in Computer Science and Automation, Microsoft Research and IMDEA, discovered the "Freak" bug in online HTTPS encrypted communications that could allow for a "man-in-the-middle" attack, where a hacker could intercept encrypted device-to-website communications if connected to the same network as the target, by degrading current TLS connections to use the now-abandoned, crackable, export-grade encryption ciphers.[67] The "Freak" bug affects only certain websites whose vulnerability is readily eliminated, but continues to potentially affect hundreds of millions of smartphone and tablet users.[68] To be sure, the U.S. encryption requirements which allowed the "Freak" exploit did not arise from a desire to create lawful exceptional access, but this example illustrates how the purposeful weakening of encryption can result in unanticipated consequences, including long-term security vulnerabilities that affect U.S. citizens and internet users around the world.

Dual_EC/Juniper, 2015: This most recent disclosure is perhaps the most directly on point, as it appears to illustrate an instance in which a high-level, U.S. government-only encryption access system was subverted by still-unknown third party actors. It is, however, worth noting that this is a developing story and, as such, the release of additional information could alter our analysis.

In 2007, the U.S. government released a new official standard for random number generators within encryption systems, Dual_EC, which was then adopted by the U.S. government and private encryption providers such as RSA, Cisco, and Juniper.[69] Shortly after the release of Dual_EC by NIST, the cryptography research community suggested that Dual_EC include a backdoor-type vulnerability, and two Microsoft employees demonstrated at a cryptography conference that "the algorithm contains a weakness that can only be described as a backdoor."[70] In 2013, disputed media reports based on the Edward Snowden leaks suggested that, while helping to develop Dual_EC, the NSA had engineered a backdoor into the algorithm that would allow for the agency to decrypt communications.[71] The Chertoff Group cannot opine on, and does not endorse this speculative theory, because it remains a classified matter. But, if it were true, this would mean that the NSA was storing a "magic number," that if revealed, would allow for the bulk decryption of U.S. corporate and (unclassified) government communications.[72] In 2013 NIST withdrew its support for Dual_EC,[73] warning against its use, and security companies subsequently examined their systems to mitigate any risks posed by the inclusion of this compromised algorithm.[74]

In 2015, Juniper disclosed that it found "unauthorized code" that created two backdoors in its NetScreen firewalls – one that would allow an attacker to gain full administrative access to the firewall and one that would allow a "passive eavesdropper to decrypt VPN traffic undetected."[75] The backdoor was specifically built to exploit the vulnerability of Dual_EC.[76] As a result, for as long as three years, an unauthorized actor – many security researchers have speculated that this may be the work of a foreign government – might have been able to decrypt Juniper traffic in the U.S. and around the world, though it is unclear whether this vulnerability was, in fact exploited.[77] As Gary McGraw, the CTO of Cigital said, "Technologists… have been warning the government for years – sometimes decades – about the hazards of backdoors like the one recently exploited in Juniper's products…Engineering a product to be secure is hard enough without intentionally designing in an Achilles' heel."[78]

We assess that the last of these examples is likely an exemplar of the driving force behind technology companies' opposition to a lawful access requirement. Some see the U.S. government itself as an at least partially malevolent actor. Major Information Technology (IT) companies seek to apply new security and encryption systems precisely because they view U.S. government access in the same light as they view access by China.[79] We do not share that viewpoint, but incidents like the Dual_EC/Juniper case undoubtedly reinforce the notion that a backdoor inserted by one country may also be exploited by others.

International Consequences of Limiting Encryption

Though our discussion is focused on the encryption debate in America, it is important to recognize that the discussion does not occur in an international vacuum. Other countries are considering the same question – with varying results and with an indeterminate effect on the American discussion.

Though our discussion is focused on the encryption debate in America, it is important to recognize that the discussion does not occur in an international vacuum. Other countries are considering the same question – with varying results and with an indeterminate effect on the American discussion. Likewise, our decisions here may have consequences overseas.

For example, some argue that American adoption of an extraordinary access requirement would encourage other countries to do the same (meaning if the US demands extraordinary access, then China will likely do the same without any restraint), while our rejection of the requirement would enable the U.S. to diplomatically oppose access requirements around the globe. If the U.S. government demands extraordinary access, even by placing the keys in escrow, how do we argue against other nations going to U.S. companies for the same access for what they believe and would describe as legitimate law-enforcement efforts?

There is, of course, good reason to think that America's decision will influence others – most notably our allies and friends. America's soft power of persuasion is most effective when it is wielded without overt hypocrisy.

There is, of course, good reason to think that America's decision will influence others – most notably our allies and friends. America's soft power of persuasion is most effective when it is wielded without overt hypocrisy.[80] At the same time, however, we should not overstate the practical significance of any decision the U.S. might make. It is uncertain that authoritarian nations (e.g. China or Russia) will forgo implementing an encryption access requirement simply because the U.S. chooses not to.

Likewise, the availability of strong encryption is sometimes seen as an integral capability for furthering American foreign policy interests. Strong encryption is often used by dissidents looking to challenge authoritarian regimes. During the Arab Spring, for example, some service providers were facing governmental demands to "unmask" the people using their systems to organize protests. The State Department was concurrently providing those same dissidents with encryption tools to help protect their anonymity.[81] The creation of a lawful access technique would make this sort of dissident empowerment more difficult to achieve.

Foreign Adoption of Access Requirements

With the foregoing in mind we, nonetheless, find it useful to briefly survey the current state of affairs regarding encryption access around the globe. In the United Kingdom, the Cameron administration introduced the Investigatory Powers Bill, which would, among other things, require companies to bypass encryption at the request of the U.K. government.[82] Under the proposal, service providers would be required to turn over communications data when served with legal notice by the government and would also be required to remove any encryption applied to the communication, effectively prohibiting providers from offering strong encryption solutions to their customers.[83]

In the aftermath of the November 13, 2015 terror attacks in Paris, the French paper *Le Monde* acquired a "wish list" purported to have been obtained from French intelligence officials outlining changes they would like to see in French law as a means of preventing such attacks in the future. The list included proposals to ban TOR, a type of free anonymizing internet software, and open Wi-Fi networks. It also included a proposal that would require service providers to provide the government with the encryption keys of its users with a court order.[84] The proposals were downplayed by the French Prime Minister, Manual Valls, who referred to the Internet as a "freedom" that allows for vital communications and "is a benefit to the economy."[85] Parliamentarians from the conservative Republican Party also introduced an amendment to the Digital Republic Bill currently under consideration by the French Parliament. The amendment would require technology companies to configure their systems such that police and intelligence agencies could always access their data, effectively banning technology companies from providing strong endpoint encryption. The stated aim of the amendment is to avoid the delay that "individual encryption systems" have on the "advancement of an investigation."[86] The French Government almost immediately rejected the amendment, calling it a "vulnerability by design" and "the wrong solution."[87]

While the Brazilian government hasn't issued any formal proposals to restrict the use of encryption for personal devices or communications, Brazilian courts have weighed in on the issue. On December 16, 2015 a Brazilian judge temporarily ordered a nation-wide ban on the widely-used smartphone application WhatsApp, which allows users to send messages via end-to-end encryption, preventing the application's makers from accessing the messages. The order was issued to punish WhatsApp for its inability to respond to a court order for the company to turn over the messages sent by WhatsApp users who were the subject of a criminal investigation by Brazilian authorities. While the ban was quickly overturned by an appeals court, the incident demonstrates the friction between Brazilian authorities and providers of encrypted communications technologies in Brazil.[88]

Meanwhile, in Australia, a new law called the Defense Trade Controls Act criminalizes the export of strong encryption technologies utilizing keys longer than 512 bits without a permit. Under the law, such technology is classified as "dual-use," meaning that it has potential military applications that subject the technology to government export restrictions. These restrictions, set to take effect in April 2016, have been criticized by some technology experts, including cryptography researchers, as overly restrictive and short-sighted.[89]

By contrast, in the Netherlands, the government has taken the opposite approach. A Dutch House of Representatives report concluded that weakening encryption products with back doors for law enforcement would leave systems vulnerable to criminals, terrorists, and foreign intelligence services. According to the position paper released in early 2016, "the use of encryption strengthens the international competitiveness

of the Netherlands and contributes to an attractive business and innovation environment for startups, data centers, and cloud computing."[90] While the report has yet to be accepted by the full general assembly, its conclusions are indicative of the varying positions of Western governments regarding encryption.

International Rights

In much of this discussion we have eschewed any reference to our reliance on underlying legal norms – for the self-evident reasons that such norms differ across the globe. It nonetheless bears mention that, at least to some degree, the use of encryption is seen internationally as a cognate protecting an individual's rights to freedom of expression and privacy. Every individual who actively uses the Internet is generally guaranteed these rights.[91] In May 2003, for example, the Committee of Ministers of the Council of Europe adopted the *Declaration on freedom of communication on the Internet* and made it clear that "in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity."[92] More recently, in May 2015, the Special Rapporteur on Freedom of Expression (FOE) reinforced the idea of the right to online anonymity and proclaimed that anonymity and encryption must be protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age.[93] UN Human Rights Chief, Navi Pillay, even went so far as to say that Internet privacy is as important as human rights.[94]

At the same time, however, as the European Court of Human Rights has pointed out, anonymity is not absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime, or the protection of the rights and freedoms of others.[95] U.S. courts have also echoed this notion and have held that "people are permitted to act pseudonymously and anonymously with each other so long as those acts are not in violation of the law."[96] Thus, to the extent relevant, encryption law and policy may need to take account of this trend in international norm setting.

Consequences – Restraining Innovation in Prospective Security

It is possible (and perhaps even highly likely) that mandating exceptional encryption access would hinder or damage innovation in the encryption technology market. It may also restrain innovation in related security technology markets. We therefore think it suitable to ask whether other security innovations will be frustrated or restrained by a duplicate key requirement or lawful access on demand.

Restraining Future Security Innovations

Implementing a backdoor for law enforcement into encryption solutions would force encryption technology providers to abandon the latest "forward secrecy" best practices for system design (a system of, in effect, one-time ephemeral encryption keys), thereby degrading the security of encryption solutions available for consumers and enterprise.

Implementing a backdoor for law enforcement into encryption solutions would force encryption technology providers to abandon the latest "forward secrecy" best practices for system design (a system of, in effect, one-time ephemeral encryption keys), thereby degrading the security of encryption solutions available for consumers and enterprise.

Currently, long-term public keys are commonly used to encrypt symmetric keys while the private key is kept in persistent storage, but this creates the risk of retrospective decryption: if an organization's private key is ever breached, all data secured with this public key (throughout the lifecycle of the key) is then immediately compromised.[97] This means that a single breakage of the private key for an e-mail server could allow for the retrospective decryption of all historical and current e-mail traffic on the server.[98]

Recognizing this inherent vulnerability, providers of encrypted communications like Google are shifting toward the method of forward secrecy, in which private keys are not kept in persistent storage – new private keys are actually generated for each new session or transaction, and then immediately discarded.[99] In keeping with forward secrecy practice, long-term keys are used only for authentication. The result of forward secrecy is that if an ill-intentioned hacker breaks a single private key, he will not be able decrypt historical

communications (because they used a different key which has since been discarded), and he will only be able to decrypt communications from this particular breached session. The attacker would theoretically have the ability to continue to decrypt communications until his breach was discovered and remediated, but he would have to break a new key for each new session he wished to decrypt. Forward secrecy enables a world in

which even then most advanced hacker can only decrypt the electronic communications of today, never accessing the electronic communications of the past.

An exceptional access system would inherently mitigate the benefits of forward secrecy. By definition, golden keys or duplicate keys in escrow are not ephemeral – they are retrospectively permanent. And so, if a private key held "in escrow" by the government or by a cooperative third party provider is ever breached, then all historical communications ever encrypted with this key are permanently compromised.[100] The access requested by law enforcement is, by definition, incompatible with forward secrecy – and would, in practice, require technology firms to abandon one of the most significant encryption security innovations of the last decade.

Creating New Risks and Vulnerabilities

While most of the encryption debate has focused on the application of cryptographic technologies to ensure confidentiality, the same technology is also used for message integrity, authentication, and non-repudiation. The latter three become much more important when cryptography is used to protect infrastructure in addition to information.

Against this backdrop, exceptional access schemes present a significant challenge: the same cryptographic keys that are used to protect confidentiality of data in systems are also used in many cases to protect and control the systems themselves.

Because there are no distinguishing features between different types of keys, most systems do not differentiate between how these keys are used. In many cases, a single key might be used for both purposes – a system that grants a third party access to read traffic and communications could also allow that third party to modify that traffic or communications.

If exploited, this could enable an attacker to leverage compromised keys to wreak havoc in a number of ways. For example, most Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) cloud offerings are administered remotely, while the security of the control traffic for these systems is managed through cryptographic keys using standard protocols like SSL/TLS. A key escrowed for the purposes of allowing access to data flowing through these systems could also allow the holder of that key to access administrative functions for that system.[101]

Moreover, as technology evolves and new systems come online – think elements of the electrical Smart Grid, driverless cars, and other "Internet of Things" applications – encryption is an essential element to ensuring the security of these cyber-physical systems. A 2009 Department of Homeland Security report detailed the importance of encryption for these purposes, but also noted the challenges it poses, stating, "Applying encryption techniques to industrial control systems can introduce significant design challenges as they add complexities and operational limitations to the environment. If not implemented correctly, an encryption system will only provide an illusion of security and could introduce risks."[102]

As we look to drive innovation and security amongst an ever-growing ecosystem of connected devices and systems, the risks to this ecosystem created by an exceptional access scheme could be significant. And while it might be theoretically possible to mitigate the impact of such a scheme by redesigning message integrity cryptographic systems from the ground up by separating them from systems used to protect confidentiality, doing so would take years, creating a significant disruption within the industry and hindering innovation.

Unanticipated Effects

Almost by definition, the unanticipated effects of a policy choice can be neither identified nor quantified. Nonetheless, we are comfortable predicting that such unanticipated effects will occur and that some of them will be adverse. Our assessment is based on the reality that the threat of malicious actors is mutating over time and that, in our experience, the pace at which the threat is mutating is accelerating. As Admiral Michael Rogers, Commander of United States Cyber Command, stated in 2015 testimony before the Senate Armed Services Committee, "we expect more nations, and even state-less groups and individuals as well, to develop and employ their own tools and cyberwarfare units to cause effects in targeted networks… (t)he cyber strife that we see now in several regions will continue to deepen in sophistication and intensity… (and) we expect state and unaffiliated cyber actors to become bolder and seek more capable means to affect us and our allies."[103] We are confident that technology companies will face new and different threats to the security of their systems and to the integrity of the services that they provide to consumers. We cannot, of course, describe that threat,

except to say with near-certainty that it will be different from the threat posed today.

And that, in turn, makes us skeptical of any fixed-point-in-time technological mandate, even one that is couched in terms of a performance objective rather than as a specific requirement for a particular technological implementation. We can, of course, imagine threat mutations that would be unaffected by a lawful access mandate. But we can also, quite readily, imagine the possibility of the development of new threat vectors for which such a mandate would be an obstacle. Candidly, in the highly dynamic, ever-changing world of cyber threats, vulnerability, and defenses, we are cautious about any governmentally-imposed obligation. In the absence of any decisive demonstration of need, our instinct is to permit the market of ideas and technological development to function without governmental interference, lest we have the collateral and unintentional effect of delaying or preventing the development of an appropriate response. Nor is our concern completely speculative. One has but to reflect on the Juniper and "Freak" incidents we discussed earlier to recognize that unintended and unanticipated consequences are an inevitable reality of government technological intervention.

Consequences – Eroding American Advantage

Adoption of an American encryption access requirement may result in adverse collateral effects, affecting the competitiveness of American businesses and U.S. national security.

American Business Opportunities Lost

The effects on American business are speculative, but likely to be quite substantial. We have (unfortunately) a test-case model for assessing how the global economy reacts to disclosures about American tech companies and access to their products afforded by the U.S. government. The revelations of NSA activity by Edward Snowden provide some indication of the rough magnitude of the effects, with estimates of economic impact on U.S. IT businesses ranging from $35 Billion[104] up to $180 Billion[105] in lost revenue over a three year period.

Perhaps more significantly, American tech companies are incurring direct costs as a result of growing concern about U.S. government access to data. Here, the evidence is anecdotal rather than systematic, but it illustrates the nature of the challenge. For example, Microsoft is building several new European Data Centers at a cost of £1.3 Billion.[106] This includes creation of a German-specific cloud to meet their concerns over U.S. activities—structured so that U.S.-based Microsoft is unable to respond to U.S. legal requests to access data in this cloud.[107] Similarly, IBM is building new data centers in London, Hong Kong, and Sydney in partial response to concerns over U.S. spying at a cost of $1.2 Billion.[108]

Finally, there is some evidence of lost business opportunities that, again, paints a grim (albeit anecdotal) picture. Germany cancelled a government telecoms contract with Verizon in June 2014 over concerns that Verizon was providing information to the U.S. government.[109] Similarly, the Brazilian government decided to move from Microsoft Outlook to an in-house solution in response to concerns over U.S. spying and access. The dollar values associated with these lost deals are not publicly known.[110] Brazil reportedly scuttled a $4.5 Billion fighter jet deal with Boeing over spying concerns, going with SAAB instead.[111] And AT&T has declined to pursue the acquisition of a European mobile provider due to concerns over U.S. spying.[112]

As we noted at the outset, the forgoing is data derived from the impute effects of concern over U.S. government access that have arisen already, mostly as the product of Edward Snowden's disclosures. These past effects are not necessarily predictive of the response to an American encryption access requirement. Indeed, they may be ameliorated somewhat by the adoption of similar access requirements in other countries. But, in our judgment, they are indicative of the likely magnitude of adverse economic effects.

National Security Effects

Perhaps the greatest harm to America that may arise from an encryption access requirement is, paradoxically, the adverse effect it would have on national security. As General Michael Hayden told the Senate Judiciary Committee in 2006: "Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge …We also need to protect that edge, and we need to protect those who provide it to us."[113] Estimates vary as to the percentage of internet traffic transiting America, but all agree that the relative volume is declining. Fears about U.S. government access will only accelerate that trend. For example, Brazil has announced its intention to build a new undersea cable to Portugal in order to avoid routing internet traffic through the U.S. (thus subjecting it

to U.S. surveillance and law enforcement). The cable will cost $185 Billion.[114]

It is equally likely that an extraordinary access requirement will drive encryption and other security technology innovation off-shore, ultimately decreasing American market share and weakening one of America's greatest built-in national security advantages. As a result, U.S. Intelligence agencies will see less traffic on American networks and have less access to the metadata associated with that traffic to the disadvantage of national security.

It is equally likely that an extraordinary access requirement will drive encryption and other security technology innovation off-shore, ultimately decreasing American market share and weakening one of America's greatest built-in national security advantages. As a result, U.S. Intelligence agencies will see less traffic on American networks and have less access to the metadata associated with that traffic to the disadvantage of national security. Again, the exact effect of an encryption access law is difficult to project, but we are comfortable predicting that it will only make other forms of intelligence analysis more difficult to accomplish, and limit the ability of the national security community to gain access to the most advanced encryption technologies for their own purposes.

Likely Effects

There are a number of practical implications and some speculation of what this transition to new "default on" encryption may mean:

- The proposed new operating systems act technologically to divest Apple and Google and others of any ability to respond to a warrant – they cannot produce what they do not have. The access question now becomes a Fifth Amendment question – whether or not the owner of the cell phone or the user who communicates or maintains encrypted cloud data can be compelled to unlock his phone or cloud storage or message by providing the passphrase. Unlike the Fourth Amendment context, this privilege is absolute. If courts recognize the Fifth Amendment protection, then the data on the phone or in the cloud is absolutely unavailable to law enforcement, even in situations in which the owner of the phone is available. This would be a significant crimp in law enforcement (or counter-terrorism) investigations.
- Notwithstanding the controversy, there may actually be less to this transition than meets the eye. The encryption default lock applies only to data on the phone itself. As we've noted before, unless the user also encrypts data before it is stored with a cloud service provider then it is the provider's encryption, not the user's, that matters. And, of course, many users store data in the cloud in an unencrypted form because they like to synchronize data across all their devices. Consumers store their data in cloud storage for the same reason. And that sort of synchronicity remains the default "on" function in both operating systems. So, all that data stored behind a hard encryption lock on a user's phone is accessible from the user's cloud storage provider as a back-up. The only way to be completely privacy protective is to turn off the cloud storage portions of a new iPhone or Android device – hardly a way to advance efficiency and productivity (and also, perhaps, a sign that law enforcement fears are overstated).
- And the same business reasons that are driving the adoption of encryption are likely to frustrate any effort to end the synchronicity default. Many tech companies make their money by offering consumers a seamless cross-platform product. And some business models involve access to consumer data for advertising purposes. We don't expect a default "off" switch for cloud storage anytime soon. To be sure, some portions of the market may move in that direction and change the basic architecture of their business model, but we suspect the transition will not be as rapid or as complete as some anticipate.

Conclusion

For the last 10 to 15 years, law enforcement has enjoyed uniquely expansive access to digital data. This reflects a relatively unique moment in time when individuals (citizens and criminals alike) have taken to using the digital domain for the creation and storage of confidential information without giving significant consideration to the security of that information. Before this era, physical security and the discontinuous nature of the kinetic domain had made practical access to stored information comparatively difficult for the government. The digital transition has, briefly, created a golden age of easy lawful access to data.

It is, to us, no surprise that the pendulum of security has begun to swing back to the more long-term norm of comparatively stronger protection of confidential information. The commercial spread of strong encryption products is but one aspect of that trend and, like most technological developments, it seems to us almost impossible to resist. Having surveyed the field extensively we are therefore convinced of the following:

- The spread of strong consumer encryption technology around the globe is inevitable;
- That spread will likely have an adverse effect on law enforcement's capacity to investigate criminal activity;
- Efforts to resist or restrain the spread of encryption technology are also likely to have adverse effects on technological development, America's international standing, and the competitiveness of its economy;
- More to the point, efforts to constrain encryption through forms of extraordinary access will inevitably introduce vulnerabilities into the security of consumer products in ways that are likely to have an adverse long-term effect on the security, privacy, and civil liberties of citizens.

We acknowledge, of course, that most of these conclusions reflect only a considered judgment of the future, not an absolute certainty. But that is the nature of public policy development. Considering all of these factors, our conclusion is that a mandate to require extraordinary lawful access to commercial encryption products would incur greater social, security, and economic costs than the benefits it would achieve. Based on what we know today from the public record, we recommend against the enactment of extraordinary lawful access requirement.

Endnotes

[1] Josh Gernstein, "FBI's James Comey: 'Venom … drained' from encryption debate," *Politico*, November 19, 2015, Accessed January 11, 2016, Available at http://www.politico.com/blogs/under-the-radar/2015/11/fbis-james-comey-venomdrained-from-encryption-debate-216090; Richard Burr, "The Debate Over Encryption: Stopping Terrorists From 'Going Dark'," *The Wall Street Journal*, December 23, 2015, Accessed January 11, 2016, Available at http://www.wsj.com/articles/stopping-terrorists-from-going-dark-1450914378.

[2] Portions of this section are adapted from Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, (Santa Barbara: Praeger, 2013), Chapter 12.

[3] Ibid, 11-12.

[4] Ibraham A. Al-Kadi, "The origins of cryptology: The Arab contributions," *Cryptologia*, 16:2 (April 1992): 97-126.

[5] For a more detailed description of public key encryption, *see* Martin Gardner, "A new kind of cipher that would take millions of years to break," *Scientific American*, Volume 237 (August 1997): 120-24.

[6] Indeed, even if private keys are still used, the size of the keys has become almost impossible to decrypt. Current standard encryption algorithms commonly use anywhere from 128 to 1024 bit keys, meaning the key is up to 1024 (4096?) bits long. At this length brute force decryption becomes practically impossible. For a 128 bit length key there are 339,000,000,000,000,000,000,000,000,000,000,000 possible keys. The number of possible keys for a 1024 bit key is much, much larger – it would take millions (generally billions) of years given today's computing power to try every possible key. That's why device encryption requiring strong authentication – such as a strong password paired with a second factor – is effectively unbreakable.

[7] To be sure, implementation is often difficult and most successful attacks against encryption take advantage of that difficulty. But as a matter of mathematics, well implemented encryption is beyond the capacity of current systems to decrypt. This may not always be the case. One caveat to the analysis in this paper is the possibility of some significant technological breakthrough that changes the dynamics of the question. For example, it is said that a working quantum computer of sufficient size would readily be capable of decrypting large prime number encryption. We leave the implications of such a development for another day.

[8] This section is adapted from Paul Rosenzweig, "Encryption Keys and Surveillance," *Lawfare*, August 5, 2013, Accessed January 11, 2016, Available at https://www.lawfareblog.com/encryption-keys-and-surveillance.

[9] "When back doors backfire," *The Economist*, January 2, 2016, Accessed January 15, 2016, Available at http://www.economist.com/news/leaders/21684783-some-spy-agencies-favour-back-doors-encryption-software-who-will-use-them-when-back.

[10] To be clear, hardware cryptomodules are not the only way to generate cryptographic keys, but they are the most commonly used approach and the most secure. See N. Sklavos, K. Touliou, and C. Efstathiou, "Exploiting Cryptographic Architectures over Hardware vs. Software Implementations: Advantages and Trade-offs," *The Proceedings of the 5th WSEAS International Conference on Applications of Electrical Engineering, Prague, Chech Republic, March 12-14, 2006* (March 2006): 147-151, Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.546.6597&rep=rep1&type=pdf.

[11] "Personal Identity Verification (PIV) of Federal Employees and Contractors," *National Institute of Standards and Technology*, Federal Information Processing Standards Publication 201-2, August 2013, Accessed January 11, 2016, Available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

[12] This solution may also be difficult to scale, but that problem of implementation is distinct from the issue of complexity eroding security that we address in the text.

[13] Clint Boulton, "Google Makes HTTPS Encryption Default for Search," *eWeek*, October 18, 2011, Accessed January 15, 2016, Available at http://www.eweek.com/c/a/Security/Google-Makes-HTTPS-Encryption-Default-for-Search-371629.; Brian Prince, "Google Gmail Switches to HTTPS to Always On by Default," *eWeek*, January 13, 2010, Accessed January 15, 2016, Available at http://www.eweek.com/c/a/Security/Google-Gmail-Switches-HTTPS-to-Always-on-by-Default-656394.

14 Timothy Seppala, "Google won't force Android encryption by default (update)," *Engadget*, March 2, 2015, Accessed January 11, 2016, Available at http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/; Andrea Peterson, "Yahoo's plan to get Mail users to encrypt their e-mail: Make it simple," *The Washington Post*, March 15, 2015, Accessed January 11, 2016, Available at https://www.washingtonpost.com/news/the-switch/wp/2015/03/15/yahoos-plan-to-get-mail-users-to-encrypt-their-e-mail-make-it-simple/; Greg Kumparak, "Apple Explains Exactly How Secure iMessage Really Is," *TechCrunch*, February 27, 2014, Available at http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/.

15 The Clipper Chip proposal was the idea that those who manufactured strong public key encryption programs should be obliged to create a master decryption key that would be stored in escrow to enable lawful access to encrypted data by law enforcement authorities. For reasons that mirror much of the current debate, that proposal was, after much discussion, shelved. For additional information see Sean Gallagher, "What the government should've learned about backdoors from the Clipper Chip," *ArsTechnica*, December 14, 2015, Accessed January 11, 2016, Available at http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

16 Ira S. Rubenstein, "Regulating Privacy by Design," *Berkley Technology Law Journal*, Volume 26 (2012): 1409.

17 Steve Lohr, "The Default Choice," *The New York Times*, October 15, 2011, Accessed January 11, 2016, Available at http://www.nytimes.com/2011/10/16/technology/default-choices-are-hard-to-resist-online-or-not.html.

18 Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review*, Volume 126, Issue 7 (May 2013): 1880-1882.

19 Lohr, "The Default Choice."

20 Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Want, "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," *Carnegie Mellon University CyLab*, October 31, 2011: 2-5, Accessed January 11, 2016, Available at https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

21 "Written Evidence (IPB0116)," *Written United Kingdom Parliamentary Evidence of Facebook Inc., Google Inc., Microsoft Inc., Twitter Inc., and Yahoo Inc*., December 21, 2015, Accessed January 11, 2016, Available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26367.html. It is, perhaps, also worth noting that for some consumers of tech products, lawful government access and use of surveillance authorities, even when transparent and enshrined in law, undermines their trust in the security of our products and services. *Id*. This post-Snowden reaction is not one that we share, generally, but it is a market-reality that is partially responsible for the development of new encryption business models in the tech industry.

22 An important caveat to this inquiry at the outset: We have limited ourselves to a discussion of matters that are in the public record and available from open sources. We acknowledge, as we must, that this inquiry necessarily excludes classified matters of which we are, by definition, unaware.

23 "Wiretap Report 2014," *United States Courts*, December 31, 2014, Accessed December 28, 2015, Available at http://www.uscourts.gov/statistics-reports/wiretap-report-2014.

24 Andy Greenberg, "Rising Use of Encryption Foiled the Cops a Record 9 Times in 2013," *Wired*, July 2, 2014, Accessed January 11, 2016, Available at http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/. We note the careful use of the word "hindered" in Mr. Vance's testimony which we read to suggest that the investigations were not frustrated completely. That aspect of the public record is worth clarifying as part of the policy development process.

25 Andy Greenberg, "Manhattan DA: iPhone Crypto Locked Out Cops 74 Times," *Wired*, July 8, 2015, Accessed December 28, 2015, Available at http://www.wired.com/2015/07/manhattan-da-iphone-crypto-foiled-cops-74-times/.

26 David Kravets, "Manhattan DA demands Congress require mobile phone backdoors," *ArsTechnica*, November 18, 2015, Accessed December 28, 2015, Available at http://arstechnica.com/tech-policy/2015/11/manhattan-da-demands-congress-require-mobile-phone-backdoors/.

27 Cyrus Vance, "DA Vance Testimony on Encryption, Technology, and Public Safety Before the United States Senate Committee on the Judiciary," *New York County District Attorney's Office*, July 8, 2015, Accessed December 28, 2015, Available at http://manhattanda.org/da-vance-testimony-encryption-technology-and-public-safety-united-states-senate-committee-judiciary.

28 We stress that our assessment of all of these is based exclusively on open source materials. As we noted earlier, classified materials to which we are, by definition, not privy, might alter the analysis.

29 Evan Perez and Shimon Prokupecz, "Paris attacker likely used encrypted apps, officials say," *CNN*, December 17, 2015, Accessed January 11, 2016, Available at http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

30 Ibid.

31 Cyrus Farivar, "Paris police find phone with unencrypted SMS saying 'Let's go, we're starting'," *ArsTechnica*, November 18, 2015, Accessed January 11, 2016, Available at http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/.

32 Joshua Kopstein, "San Bernardino Shooters' Phone Had 'Built in Encryption, Just Like Every Phone," *Motherboard*, December 12, 2015, Accessed January 11, 2016, Available at http://motherboard.vice.com/read/san-bernardino-shooters-phones-had-built-in-encryption-just-like-every-phone.

33 Ibid.

34 Of course, more prominently, the news has reported that one attacker advocated violent jihad on multiple channels that would have been accessible to U.S. intelligence officials with proper warrants, including emails, private Facebook messages to Pakistani friends and posts on dating websites. None of these channels was reported to have been encrypted. See Matt Apuzzo, Michael S. Schmidt, and Julia Preston, "U.S. Visa Process missed San Bernardino Wife's Online Zealotry," *The New York Times*, December 12, 2015, Accessed January 11, 2016, Available at http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=1.

35 James B. Comey, "Statement of James B. Comey, Director, Federal Bureau of Investigation, Before the Committee on The Judiciary, United States Senate, for a hearing regarding Oversight of the Federal Bureau of Investigation," *Committee on The Judiciary, United States Senate*, December 9, 2015, Accessed January 11, 2016, Available at http://www.judiciary.senate.gov/imo/media/doc/12-09-15%20Comey%20Testimony.pdf.

36 Telegram is a non-commercial messaging application that purports to maintain the complete privacy of conversations that use the application. *See* https://telegram.org/.

37 Rita Katz, "Jihadist are making their plans public. Why hasn't the FBI caught on?," *The Washington Post*, December 17, 2015, Accessed January 11, 2016, Available at https://www.washingtonpost.com/news/in-theory/wp/2015/12/17/jihadists-are-making-their-plans-public-why-hasnt-the-fbi-caught-on/.

38 David Inserra, "An Interactive Timeline of Islamist Terror Plots Since 9/11," *The Daily Signal*, September 10, 2015, Accessed January 11, 2016, Available at http://dailysignal.com/2015/09/10/a-timeline-of-73-islamist-terror-plots-since-911/.

39 Ibid.

40 Ibid.

41 Pamela Brown and Jim Sciutto, "U.S. law enforcement thwarted plots timed to July 4," *CNN*, July 10, 2015, Accessed January 11, 2016, Available at http://www.cnn.com/2015/07/09/politics/july-4-terror-plot-law-enforcement/.

42 We know of no public open sources that report the success of key-logger attacks on terrorist activity (capturing the encryption passwords or unencrypted text before encryption). We assume, however, that such capabilities exist and have been deployed by law enforcement and the intelligence community.

43 *United States v. John Doe*, 11-12268 & 11-15421 (2011), Available at https://www.eff.org/files/filenode/opiniondoe22312.pdf.

44 *Commonwealth vs. Leon I. Gelfgatt*, SJC-11358 (2015), Available at http://www.suffolk.edu/sjc/archive/opinions/SJC_11358.pdf.

45 *Virginia v. Baust*, CR-14-1439 (2014), Available at https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2014/11/SKMBT_C364e14103109110.pdf.

46 Paul Tassi, "How ISIS Terrorists May have used PlayStation 4 To Discuss And Plan Attacks," *Forbes*, November 14, 2015, Accessed January 11, 2016, Available at http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/.

47 Jaikumar Vijayan, "The NSA tracks World of Warcraft and other online games for terrorist clues," *Computerworld*, December 9, 2013, Accessed January 11, 2016, Available at http://www.computerworld.com/article/2486632/cyberwarfare/the-nsa-tracks-world-of-warcraft-and-other-online-games-for-terrorist-clues.html.

48 Paul Tassi, "How ISIS Terrorists."

49 Beatrice Berton, "The dark side of the web: ISIL's one-stop shop?," *European Union Institute for Security Studies*, Alert Number 30, June 26, 2015, Accessed January 11, 2016, Available at http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf.

50 Natasha Bertrand, "ISIS is taking full advantage of the darkest corners of the Internet," *Business Insider*, July 11, 2015, Accessed January 11, 2016, Available at http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7.

51 Nate Anderson, "Times Square bombing suspect used a 'burner' phone," *ArsTechnica*, May 5, 2010, Accessed January 11, 2016, Available at http://arstechnica.com/tech-policy/2010/05/times-square-bombing-suspect-used-a-burner-phone/.

52 Evan Perez and Shimon Prokupecz, "Paris attackers likely used."

53 Greg Miller and Julie Tate, "Months before U.S. raid, Bin Laden considered leaving Pakistan compound," *The Washington Post*, May 20, 2015, Accessed January 11, 2016, Available at https://www.washingtonpost.com/world/national-security/us-opens-files-on-osama-bin-ladens-private-library/2015/05/20/7f7949b8-fef7-11e4-833c-a2de05b6b2a4_story.html.

54 See Director Comey's response to Senator Lee's (R-UT) question from the Senate Committee on the Judiciary Federal Bureau of Investigation Oversight hearing on December 9, 2015, Timestamp is approximately 1:24:00, Available at http://www.c-span.org/video/?401606-1/fbi-director-james-comey-oversight-hearing-testimony#.

55 Alessandria Masi, "ISIS Bans Apple iPhones, iPads, iPods In The Caliphate Due To Fears They're Being Tracked," *International Business Times*, February 6, 2015, Accessed January 11, 2016, Available at http://www.ibtimes.com/isis-bans-apple-iphones-ipads-ipods-caliphate-due-fears-theyre-being-tracked-1807006.

56 David E. Sanger and Nicole Perlroth, "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist," *The New York Times*, December 9, 2015, Accessed January 11, 2016, Available at http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html.

57 Margaret Coker, Danny Yadron, and Damian Paletta, "Hacker Killed by Drone Was Islamic State's 'Secret Weapon,'" *The Wall Street Journal*, August 27, 2015, Accessed January 11, 2016, Available at http://www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560.

58 Rita Katz, "Jihadist are making their plans public."

59 ""How Al-Qaeda Uses Encryption Post-Snowden (Part 1)," *Recorded Future*, May 18, 2014, Accessed January 11, 2016, Available at https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/.

60 Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, matt blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landu, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael specter, and Daniel J. Weitzner, "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," *Massachusetts Institute of Technology*, Computer Science and Atificial Intelligence Laboratory Technical Report (July 6, 2015): 8, Accessed January 11, 2016, Available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

61 Herb Lin, "Making Progress on the Encryption Debate," *Lawfare*, February 24, 2015, Accessed January 11, 2016, Available at https://www.lawfareblog.com/making-progress-encryption-debate.

62 Matt Blaze, "A key under the doormat isn't safe. Neither is an encryption backdoor," *The Washington Post*, December 15, 2015, Accessed January 11, 2016, Available at https://www.washingtonpost.com/news/in-theory/wp/2015/12/15/how-the-nsa-tried-to-build-safe-encryption-but-failed/.

63 Harold Abelson, et al., "Keys Under Doormats": 17.

64 Harold Abelson, et al., "Keys Under Doormats": 9.

65 Kim Zetter, "RSA Agrees to Replace Security Tokens After Admitting Compromise," *Wired*, June 7, 2011, Accessed January 11, 2016, Available at http://www.wired.com/2011/06/rsa-replaces-securid-tokens/.

66 David Gilbert, "What is Freak? Security bug affects hundreds of millions of iPhone, iPad and Android users," *International Business Times*, March 4, 2015, Accessed February 7, 2016, Available at http://www.ibtimes.co.uk/what-freak-security-bug-affects-hundreds-millions-iphone-ipad-android-users-1490379.

67 David Gilbert, "What is Freak?"

68 David Gilbert, "What is Freak?"

69 Kim Zetter, "Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA," *Wired*, December 22, 2015, Accessed January 11, 2016, Available at http://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/.

70 Bruce Schneier, "The Strange Story of Dual_EC_DRBG," *Schneier on Security*, November 15, 2007, Accessed January 11, 2016, Available at https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html.

71 Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham, "On the Practical Exploitability of Dual EC in TLS Implementations," *DualEC.org*, June 6, 2014, Accessed January 11, 2016, Available at http://dualec.org/DualECTLS.pdf.

72 Nicholas Weaver, "A Tale of Three Backdoors," *Lawfare*, August 27, 2015, Accessed January 11, 2016, Available at https://www.lawfareblog.com/tale-three-backdoors.

73 "Supplemental ITL Buletin for September 2013," *National Institute for Standards and Technology*, September 2013, Accessed January 13, 2016, Available at http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf.

74 Kim Zetter, "Researchers Solve Juniper."

75 Peter Loshin, "Juniper firewall backdoors add fuel to encryption debate," *TechTarget*, December 23, 2015, Accessed January 11, 2016, Available at http://searchsecurity.techtarget.com/news/4500269299/Juniper-firewall-backdoors-add-fuel-to-encryption-debate.

76 It is possible that the vulnerability discovered in the code is a "bug" instead of a "backdoor." Bugs and backdoors are functionally identical, the difference between the two being intent. While we cannot definitively prove the intent of the coders responsible for this vulnerability, we share the general consensus that this particular vulnerability is more likely to be a backdoor rather than a bug.

77 Matthew Green, "On the Juniper backdoor," *A Few Thoughts on Crytograph Engineering Blog*, December 27, 2015, Accessed January 11, 2016, Available at http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html.

78 Peter Loshin, "Juniper firewall backdoors."

79 Perhaps more to the point, so does their global consumer base. In a post-Snowden world the business necessity of adopting encryption technology and treating US government access as similar to that of other governments is palpable.

80 Henry Farrell and Martha Finnemore, "The End of Hypocrisy," *Foreign Affairs*, November/December 2013, Accessed January 11, 2016, Available at https://www.foreignaffairs.com/articles/united-states/2013-10-15/end-hypocrisy.

81 Andrea Peterson, "The NSA is trying to crack Tor. The State Department is helping to pay for it," *The Washington Post*, October 5, 2013, Accessed January 11, 2016, Available at https://www.washingtonpost.com/news/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/.

82 "Draft Investigatory Powers Bill," *Secretary of State for the Home Department*, November 2015, Accessed December 28, 2015, Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

83 Tom Whitehead, "Internet firms to be banned from offering unbreakable encryption under new laws," *The Telegraph*, November 2, 2015, Accessed December 28, 2015, Available at http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html.

84 Laurent Borredon, "A Beauvau, certains vourdraient interner les fiches," *Le Monde*, December 5, 2015, Accessed December 28, 2015, Available at http://www.lemonde.fr/attaques-a-paris/article/2015/12/05/la-liste-musclee-des-envies-des-policiers_4825245_4809495.html; Tim Cushing, "French Law Enforcement 'Wishlist' Includes Banning Open WiFi, Tor Connections And Encrypted Communications," *TechDirt*, December 7, 2015, Accessed December 28, 2015, Available at https://www.techdirt.com/articles/20151206/08095333001/french-law-enforcement-wishlist-includes-banning-open-wifi-tor-connections-encrypted-communications.shtml.

85 Lucian Armasu, "French PM Seems to Realize Banning Encrypted Comms Could Hurt Economy, Security," *Tom's Hardware*, December 10, 2015, Accessed December 28, 2015, Available at http://www.tomshardware.com/news/france-backtracks-tor-wi-fi-ban,30731.html.

86 Patrick Howell O'Neill, "French government considers law that would outlaw strong encryption," *The Daily Dot*, January 12, 2016, Accessed January 13, 2016, Available at http://www.dailydot.com/politics/encryption-backdoors-french-parliament-legislation-paris-attacks-crypto-wars/.

87 Glyn Moody, "French Government rejects crypto backdoors as 'the wrong solution,'" *ArsTechnica*, January 14, 2016, Accessed January 14, 2016, Available at http://arstechnica.co.uk/tech-policy/2016/01/french-government-rejects-crypto-backdoors-as-the-wrong-solution/.

88 Elia Groll, "Why did Brazil Block WhatsApp?," *Foreign Poilcy*, December 17, 2015, Accessed December 28, 2015, Available at http://foreignpolicy.com/2015/12/17/why-did-brazil-block-whatsapp/.

89 Juha Saarinen, "Experts protest Aussie law banning crypto export," *itNews*, July 13, 2015, Accessed December 28, 2015, Available at http://www.itnews.com.au/news/experts-protest-aussie-law-banning-crypto-export-406439.

90 "Kabinetsstandpunt encryptie," *Tweede Kamer Der Staten-Generaal*, January 4, 2016, Accessed January 11, 2016, Available at http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015; An unofficial translation is available at the *Cyberwar Blog* at https://blog.cyberwar.nl/2016/01/full-translation-of-the-dutch-governments-statement-on-encryption/.

91 "Right to Online Anonymity," *Article 19*, June 2015, Accessed January 11, 2016, Available at https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

92 Ibid.

93 Ibid.

94 Haroon Siddique, "Internet privacy as important as human rights, says UN's Navi Pillay," *The Guardian*, December 26, 2013, Accessed January 11, 2016, Available at http://www.theguardian.com/world/2013/dec/26/un-navi-pillay-internet-privacy.

95 "Right to Online Anonymity," *Article 19*.

96 *Columbia Ins. Co. v. seescandy.com,* 185 F.R.D. 573, 578 (N.D. CA 1999), Available at https://cyber.law.harvard.edu/property00/domain/Sees.html.

97 Harold Abelson, et al., "Keys Under Doormats": 12.

98 Adam Langley, "Protecting data for the long term with forward secrecy," *Google Online Security Blog*, November 22, 2011, Accessed January 11, 2016, Available at https://googleonlinesecurity.blogspot.com/2011/11/protecting-data-for-long-term-with.html.

99 Ibid.

100 Harold Abelson, et al., "Keys Under Doormats": 12.

101 Note that these systems are already coming under attack through other means (as the Internet Engineering Task Force (IETF) documented last year at https://tools.ietf.org/html/rfc7457); escrowed keys could create a new attack vector.

102 "Department of Homeland Security: Control Systems Communications Encryption Primer," *Department of Homeland Security, Control Systems Security Program, national Cyber Security Division*, December 2009, Accessed January 19, 2016, Available at https://ics-cert.us-cert.gov/sites/default/files/documents/Encryption%20Primer%20121109.pdf.

103 Admiral Michael Rogers, "Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," *Senate Committee on Armed Services*, March 19, 2015, Accessed February 8, 2016, Available at http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf.

104 Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?," *The Information Technology & Innovation Foundation*, August 2013, Accessed January 11, 2016, Available at http://www2.itif.org/2013-cloud-computing-costs.pdf.

105 James Staten, "The Cost of PRISM Will Be Larger than ITIP Projects," *Forrester*, August 14, 2013, Accessed January 11, 2016, Available at http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

106 Peter Bright, "Microsoft to offer UK-based Azure, Office 365 from late 2016," *ArsTechnica UK*, November 11, 2015, Accessed January 11, 2016, Available at http://arstechnica.co.uk/information-technology/2015/11/microsoft-to-offer-uk-based-azure-office-365-from-late-2016/.

107 Glyn Moody, Microsoft building data centers in Germany that US government can't touch," *ArsTechnica*, November 12, 2015, Accessed January 11, 2016, Available at http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/.

108 Claire Cain Miller, "Revelation of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014, Accessed January 11, 2016, Available at http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

109 Jeevan Vasagar, "Berlin drops Verizon over US spying fears," *The Financial Times*, June 26, 2014, Accessed January 11, 2016, Available at http://www.ft.com/cms/s/0/93f6b66e-fd4f-11e3-96a9-00144feab7de.html.

110 Angelica Mari, "Brazilian government to ditch Microsoft in favour of bespoke email system," *ZDNet*, October 14, 2013, Accessed January 11, 2016, Available at http://www.zdnet.com/article/brazilian-government-to-ditch-microsoft-in-favour-of-bespoke-email-system/.

111 Kim Zetter, "Personal Privacy is only one of the costs of NSA Surveillance," *Wired*, July 29, 2014, Accessed January 11, 2016, Available at http://www.wired.com/2014/07/the-big-costs-of-nsa-surveillance-that-no-ones-talking-about/.

112 Anton Troianovski, Thomas Gryta, and Sam Schechner, "NSA Fallout Thwarts AT&T," *The Wall Street Journal*, Accessed January 11, 2016, Available at http://www.wsj.com/news/articles/SB10001424052702304073204579167873091999730.

113 John Markoff, "Internet Traffic Begins to Bypass the U.S.," *The New York Times*, August 29, 2008, Accessed January 11, 2016, Available at http://www.nytimes.com/2008/08/30/business/30pipes.html?pagewanted=print&_r=0.

114 Kathleen Culderwood, "Brazil Builds Internet cable To Portugal To Avoid NSA Surveillance," *International Business Times*, November 1, 2014, Accessed January 11, 2016, Available at http://www.ibtimes.com/brazil-builds-internet-cable-portugal-avoid-nsa-surveillance-1717417.

About The Chertoff Group

The Chertoff Group is a premier global advisory firm focused on security and risk management. Founded in 2009, The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions, and risk management security services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantages. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group maintains offices in Houston, London, Menlo Park, and New York City. For more information about The Chertoff Group, visit **www.chertoffgroup.com**.

THE CHERTOFF GROUP

www.chertoffgroup.com