COLUMBIA LAW SCHOOL

YALE LAW

CENTER FOR ADVANCED STUDIES ON TERRORISM · CAST ·

Going Dark

Implications of an Encrypted World

www.terrorstudies.org

Contents

Foreword and Acknowledgements

The movement from an analog world to a digital one is a fact of modern life; people have much less control over their personal data or what is done with their data. Paper files and other antiquated media have been replaced by digital files, servers and devices of all kinds. Leaks and media reports have made it clear that information flowing through these systems is vulnerable to "hacks," surveillance programs and commercial data exploitation. Unauthorized access to data has gone beyond benign or embarrassing breaches to serious criminal behavior producing substantial economic loss. Non-state actors and hostile countries are endangering the nation's security and its political process.

As a result of this increased awareness and actual damage, users are demanding greater privacy and security. Commercial suppliers of devices and software have moved to meet this demand with new products employing various encryption schemes and other security features. They continue to do so at a time when the available technology supports increasingly effective encryption and when the legal regime can no longer control its application. In most cases, the new types of protection can be provided to users at zero marginal cost and free from any effective restrictions other than possible export control.

Terrorists increasingly utilize commercially available encrypted communication apps to escape surveillance and reduce their vulnerabilities – intelligence systems have much less ability to illuminate these activities, leading to the metaphor of the world "going dark." This paradigm shift has given rise to a debate within the government, academic community and media over what "going dark" really means and how it affects national security. Clearly these technologies raise questions about how to ensure required and legitimate government access to data in areas such as intelligence and law enforcement

The present analysis is the work of a study team including national security specialists, legal authorities, and cyber-security professionals examining the broad set of policy, legal, economic and technological issues involved. It does so recognizing that there are major dynamics involved, and the world of today will not be the same in ten years, five years, or even one year. User demands, the technologies, and the legal regime are all changing rapidly.

The world remains on a technology path that cannot be stopped, and the implications of an increasingly encrypted world must be seen in this evolving context. This study is intended to present a fair view of what the path may be in these critical areas, as well as what practical options might exist. It also attempts to place these options within the context of a legal regime that is evolving, both domestically and internationally. Statutes, case law, and international agreements are all attempting to grapple with the new technologies and user demands for greater privacy and security.

This study effort was made possible with support from the Center for Advanced Studies on Terrorism (CAST) and the Defense Advanced Research Projects Agency (DARPA). The views expressed are only those of the individual study team members and in no way are intended to reflect the views of any organization or the U.S. Government. The study team also acknowledges Columbia Law School's assistance in making available the facilities and support staff for study team meetings.

The study team has also benefited greatly from the work of several research assistants, currently students at Columbia Law School and Yale Law School, as well as insightful comments and suggestions from various individuals with extensive government experience who have been generous enough to review earlier drafts of this report and provide their insight.

New York, N.Y. – April 2017

Lillian Ablon
David Aitel
Sofia d'Antoine
Edward Doyle
Thomas Garwin
Daniel Guido
Nicholas Rostow
Mara Tam
Ryan Stortz
Abraham Wagner
Kevin Yorke

Executive Summary

The digital revolution has created a world where analog paper files and other antiquated media have largely been replaced by digital data. Neither the government nor the private sector anticipated the speed of this technological revolution, nor did they anticipate demands for privacy and security, or provide adequate technical solutions in a timely manner. In the digital world, users are no longer in control of their personal data or what is being done with it, and are increasingly demanding levels of privacy and security that simply did not exist before. Often users look to technical solutions, such as encryption, as an effective means of meeting this challenge. As an unintended result, criminals and hostile actors face greatly reduced costs in hiding their activities from legitimate U.S. Government surveillance, effectively "going dark."

Solving the Cybersecurity Problem: In today's world, cybersecurity must be an active process rather than a passive condition. In the coming years many of the more glaring vulnerabilities that currently exist will be eliminated, both because users are now demanding it and technical solutions can be implemented to deal with the some of the known and evolving vulnerabilities. Vulnerable old Internet protocols developed in the 1960s will be patched, supplemented, and eventually replaced while a more serious approach to securing devices and servers against cyber threats will be undertaken by the government and commercial service providers. At the same time, virtually all software systems are inherently vulnerable to either technical attacks, social engineering or insider activity. Malicious exploits will always be developed to attack new software creating an ongoing challenge.

The Changing Legal Regime: An earlier legal regime that permitted controls over encryption technology is no longer viable. Recent controversies include proposed solutions that would force companies to enable government access to user data pursuant to legal process, though companies may take action to make access impossible. Thus far, no such solutions have been enacted in the U.S. although proponents continue to press for them under the belief that Congress can legislate effective solutions in a world market over which it has no actual control.

The Ongoing Debate Over Going Dark: Greatly increased use of encryption technology, often referred to as "going dark," is a double-edged sword. The technology provides needed levels of privacy and security, but also presents a major challenge for intelligence services and law enforcement authorities seeking legitimate access to communications and data files. The U.S. Intelligence and law enforcement communities, as well as the media and others, are engaged in an ongoing debates about the use of encryption; what "going dark" means in technical and legal terms; what impact it will have on their respective operations; and what can be done to mitigate the problem. At the center of this debate is encryption technology impeding lawful intercept operations within even the most stringent interpretations of the Fourth Amendment right to privacy. Various technical and legal "solutions," have been proposed, but their effectiveness over the long run remains uncertain. Some scholars are of the opinion that the issue will resolve itself, however many lead technologists and lawyers argue compellingly that the problem is far from trivial. The most significant factors include:

- ***A New Paradigm for User Demand:*** In the digital world where users are no longer in control of their data, users are now demanding technical solutions. Driving this demand is an increasing awareness of vulnerabilities, "hacks," and leaks about surveillance programs, which has accelerated the process.
- ***Encryption is Now Entirely in Software:*** Encryption no longer requires costly electromechanical devices and in many cases does not require specialized chips, although some devices now employ a co-processor to handle crypto functions for security reasons. All devices, from smartphones to large computers, contain powerful processors. At the same time, secure encryption algorithms are readily available, and the marginal cost of employing encryption technology has fallen to zero.
- ***The U.S. Cannot Control a World Problem:*** Any effort by Congress to force companies to provide continued access to user data is doomed to fail, as suppliers outside the U.S. are not subject to U.S. law and court order. A legal regime that enabled the U.S. to control both encryption research and security technology as an arms export is long past and cannot be restored. Attempts to counter these facts are only likely to disadvantage U.S. firms and people in a very competitive world.

- ***Privacy is Winning in the Legal Regime:*** Privacy advocates have been fighting a relentless legal battle in the courts to extend Fourth and Fifth Amendment constitutional protections to important national security programs. By and large, they are winning and will continue to do so in Congress, the federal courts and the Supreme Court.
- ***Technical Solutions May Be Marginal:*** The Intelligence Community has vast resources, but cannot perform miracles. The concept of implementing backdoors, exploits, and other technical solutions on a large scale may not be realistic in the long run. Development of new exploits by the NSA and others will become a more difficult and costly enterprise.

Focus on the Technology Path: It is essential to recognize that the world of cyber technology is dynamic and that the trends outlined are destined to continue. Too often analyses focus only on the current state of affairs. In considering the issues of privacy, security and encryption, it is even more important to think about scenarios five and ten years into the future. User demands for privacy and security will certainly grow over the coming decade, while the technologies that enable both encryption and other aspects of cybersecurity will continue to improve. Stopping these trends, or working around them, either through legal or technical means may not be a viable long-term solution. Many of the current cybersecurity problems will be solved a decade from now, but new ones are certain to emerge. Here both the government and industry must meet to solve evolving demands.

These are challenging prospects to the needs of the Intelligence Community and law enforcement authorities. There is already a dynamic tension between "solutions" that deny access to data to all but the user and recipient, increased use of encryption, and technical means to work around these solutions. The needs and desires of the intelligence community and law enforcement, however, are not going to prevent the world from "going dark" in many respects, and they may in fact need to look to other means for solving their legitimate requirements. Here there remain many open questions to which there are currently no perfect answers.

1. Introduction—Impact of the Digital Revolution

The digital revolution cannot be reversed. Clearly the world will not return to analog files and other antiquated media. While few anticipated the speed or magnitude of this information and communication technology revolution, neither the government nor the private sector fully anticipated user demands for privacy and security, nor did they provide adequate technical solutions in a timely manner. In the digital world, users are no longer in control of their personal data, or what is being done with it, and they are responding to this increased vulnerability by demanding higher levels of digital privacy and security.[1] It is not surprising that users are looking to technical solutions employing encryption as an effective means of meeting this challenge.

The Ongoing Debate Over Going Dark: The U.S. intelligence and law enforcement communities, as well as the media and others, are engaged in an ongoing debate about the use of encryption, what "going dark" means in technical and legal terms, what impact it will have on their respective operations, and what can be done to mitigate the problem.[2] At the center of this debate is the use of encryption technology and related security safeguards which stand to impede lawful intercept operations meeting even the most stringent interpretations of the Fourth Amendment right to privacy.[3]

While the earlier legal regime that permitted controls over encryption technology is no longer viable, various proposed solutions force companies to enable the government to access user data pursuant to legal process, if, indeed, it will even be possible for companies to do so. Thus far, no such solutions have been enacted in the U.S. although proponents continue to press for them under the belief that Congress can legislate effective solutions in a world market over which it has no control.

Distinct from the debate surrounding lawful intercept operations are the technical questions of whether modern encryption solutions are truly safe and whether the U.S. and other intelligence services will ultimately be able to "hack" around them. While there are

[1] This is the beginning of a debate over what is known as the "third party" doctrine. See, for example, Jay Stanley, *Reviving the Fourth Amendment and American Privacy* (American Civil Liberties Union, 2010).

[2] For one recent and relatively comprehensive analysis, see *Don't Panic: Making Progress on the "Going Dark Debate,* (The Berkman Center for Internet and Society at Harvard University, February 2016). See also *Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext* (National Academies Press, 2016).

[3] Without continued access to communications and data related to terrorist and criminal activities, for example, intelligence and law enforcement will be severely hampered in performing these critical missions. There is increasing evidence that ISIS and other terrorist organizations use encrypted communications.

arguments on both sides of this issue, the balance favors encryption technology which continues to improve and has become essentially cost-free in marginal terms.

Solving the Cybersecurity Problem: The development of cybersecurity solutions is an ongoing process. In the coming years many of the more glaring vulnerabilities that currently exist will be eliminated, both because users are now demanding it and because technical solutions can be implemented to deal with the some of the known and evolving vulnerabilities.[4] Vulnerable old Internet protocols developed in the 1960s will most likely be patched and supplemented by more secure approaches and eventually replaced entirely, while a more serious approach to securing devices and servers against cyber threats will be undertaken by the government and commercial service providers. A central requirement of meeting the security challenges involves the use of encryption technologies at various points in the process.

For decades the widespread use of these technologies has faced technical, economic and legal barriers in the U.S. and elsewhere. Technical impediments prior to an all-digital era required costly electromechanical devices to do both analog to digital conversion as well as encryption. In the legal domain, the government sought to control encryption research, the export of encryption technology, and specific aspects of allowable systems such as key length and control. These technical and legal impediments are no longer of strategic value for the nation, and in fact, are detrimental in many highly important areas, including ongoing commerce and national security.

The New Paradigm – Users Are Not in Control: Previously the "analog world" was one where users had actual control of their data, which resided in paper files and on other physical media.[5] Increasingly, user data is in third party hands, and users have no choice in the matter, and often have no say over what those who do hold their data can do

[4] Most experts agree that cybersecurity problems will not be totally solved in any relevant time frame, and most likely never. Software imperfections and the technical exploits developed to take advantage of them will always exist. The need for legitimate users to access data remotely inevitably produces "social engineering" vulnerabilities where intruders can impersonate legitimate users. Insiders with access to information will always be able to remove information to some degree. At the same time, many of the most troublesome vulnerabilities can be addressed effectively. However, precisely how this will be accomplished and who will bear the costs remain to be seen. By most estimates implementing effective solutions to this set of problems is certainly less costly than getting to the moon was years ago, or getting to Mars as has been proposed.

[5] They might also have existed as digital media in a user's home or office. However, these were not connected to any network.

with it.[6] The demand for encryption and related technology was either limited or not sufficiently compelling that commercial suppliers were willing to fight this battle. Historically, encryption and cryptographic systems were largely used by the military and intelligence services.[7] Virtually all efforts to sell encryption devices as commercial products failed because users had little to secure and limited incentive to bear the high cost or inconvenience of the systems available.

With the transition to the "digital world," users have lost almost all control of their data as their communications and data storage have become increasingly vulnerable unless they actively use protective technologies.[8] For example, users were given no choice in the matter when personal financial and health records were migrated to computer systems connected to networks. Now criminals and non-state actors, such as terrorist groups, have moved into cyberspace with a vengeance and actively seek this data.[9] New technologies have evolved and costs, including legal barriers to encryption, have become negligible. Publicity surrounding government surveillance programs has also accelerated the process.[10] It is not surprising that commercial suppliers are moving to meet this increasing demand.

---

[6] Financial and medical records are only the tip of the iceberg: personal communications and data on commercial servers have also grown exponentially.

[7] Systems developed after World War I, for example, were costly, cumbersome, and inconvenient. Most were complex electromechanical devices that used vacuum tube circuits, rotors and other high precision mechanical parts. Their use generally required a trained operator as well. Even large commercial firms were unwilling to bear the costs.

[8] As noted, financial and health service providers have moved to electronic record systems and all are online. Where users still have some choice, such as in the use of paper "snail mail," as a practical matter users have largely preferred e-mail, text messaging, and social media.

[9] See, for example, "Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependent on Aps, Software – Kik, Surespot, Telegram, Wickr, Detekt, Tor," *Inquiry & Analysis Series Report No. 1168,* Middle East Media Research Institute (MEMRI)(June 16, 2015); Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* (June 2016); and Sam Schechner and Benoit Faucon, "New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent, *The Wall Street Journal* (September 11, 2016). It is widely believed that Tor and Telegram can currently be accessed, while the others present a more difficult challenge.

[10] Director of National Intelligence, James Clapper, has recently stated that the process has been greatly accelerated. See, Jenna McLaughlin, "Spy Chief Complains The Edward Snowden Sped Up Spread of Encryption by 7 Years," *The Intercept* (April 25, 2016). It is unclear where Director Clapper came up with the seven-year figure, but there is widespread agreement with his assessment that the trend has accelerated.

Is the World Really "Going Dark?" Greatly increased use of encryption technology, often referred to as "going dark," is a double-edged sword. The technology provides needed levels of privacy and security, but also presents a major challenge for intelligence services and law-enforcement authorities seeking legitimate access to communications and data files for purposes that most agree are in the public good. Those involved in studies of the issue have proposed various legal and technical "solutions" although their effectiveness remains open to question. While the debate continues, a number of key factors argue compellingly that the problem is far from trivial and not "overhyped," as some have suggested.[11] The most significant factors include:

- ***A New Paradigm for User Demand:*** In the digital world, users now no longer control their data and are demanding technical solutions. Driving this demand is an increasing awareness of vulnerabilities, "hacks," and leaks about surveillance programs such as those from former NSA contractor Edward Snowden. These developments have accelerated the demand and awareness by years.
- ***Encryption is Now Entirely in Software:*** Encryption no longer requires costly electromechanical devices and in many cases does not require specialized chips.[12] All devices, from smartphones to large computers, contain powerful processors that continue to grow even more powerful. At the same time, secure encryption algorithms are readily available worldwide and cannot be controlled. Even better algorithms will become available over the coming decade while the marginal cost of employing encryption technology has effectively fallen to zero. At the same time, cost of creating the better encryption is not zero and this may slow down the proliferation of encryption. Given enough time, technologists will be able to circumvent the existing exploits. In addition, as more sensitive

[11] Those who see the problem as "overhyped" include Prof. Jonathan Zittrain of Harvard and DNI Director James Clapper. Among those taking a different view and see "going dark" as a far more serious problem are FBI Director James Comey and Congressman Adam Schiff, Ranking Minority Member of the House Permanent Select Committee on Intelligence (HPSCI).

[12] In some areas specialized chips are utilized, such as AES-NI, high performance applications, secure enclave and hardware acceleration of algorithms, key management, and HSM's. The software/hardware exploitation of these implementations also pose a concern, such as bad HWRNG's. There are also custom made co-processors to handle crypto functions off the main CPU for security reasons, some of which are actually using formally verified software/hardware implementations.

information is stored using the same encryption techniques that are widely available, the higher the incentive is to find a hack.

- ***The U.S. Cannot Control a World Problem:*** Any effort by Congress to force companies to provide continued access to user data is doomed to failure, as suppliers outside the U.S. are not subject to U.S. law and court order.[13] An earlier legal regime that enabled the U.S. to control not only encryption research but also security technology as an arms export is long past and cannot be restored.

- ***Privacy is Winning in the Legal Arena:*** Privacy advocates have been fighting a relentless battle in the courts to extend Fourth and Fifth Amendment Constitutional protections to important national security programs, such as Sections 215 of the USA Patriot Act and 702 of the FISA Amendments Act of 2008, and more recently FBI efforts to "unlock" iPhones in criminal cases.[14] By and large, privacy advocates are winning and will continue to do so in Congress, the federal courts and the Supreme Court.

- ***Technical Solutions May Be Marginal:*** The Intelligence Community has vast resources and technical skills, but cannot perform miracles. The concept of implementing backdoors, exploits and other technical solutions on a large scale may not be realistic, particularly in the long run.[15] As the world becomes increasingly flooded with zettabytes of encrypted digits exploits by NSA and others that may be possible now, will become more difficult. These exploits are costly enterprises dependent on finding new software vulnerabilities and user error, or covert operations. The "golden age of SIGINT" may be over, particularly within the next five to ten years.

---

[13] See, for example, "Proposed State Bans on Phone Encryption Makes Zero Sense," *Wired* (January 16, 2016). One legislative attempt to deal with the problem is the proposed *Compliance with Court Orders Act of 2016*, otherwise known as the Burr/Feinstein draft, which also makes little sense and is unlikely to be enacted into law.

[14] See Ashley Gorski and Patrick C. Toomey, *Unprecedented and Unlawful: The NSA's "Upstream" Surveillance* (American Civil Liberties Union, September 19, 2016).

[15] DNI Director James Clapper's remark that we have always been able to break into encrypted system and will always be able to do so is both inaccurate and unrealistic. Soviet use of "one time pads" in Afghanistan presented an insurmountable challenge to NSA in the 1979 time frame. To the extent that modern cryptographic systems become electronic equivalents of the one-time pad, breaking into them outright is a formidable challenge indeed. See, McLaughlin, *op cit*.

Focus on the Technology Path: It is essential to recognize that the cyber world is a dynamic one and that the trends outlined are destined to continue. Too often analyses focus only on the current state of affairs. Considering the issues of privacy, security and encryption, it is even more important to think about scenarios five and ten years into the future. User demands for privacy and security will certainly grow over the coming decade, while the technologies that enable both encryption and other aspects of cybersecurity will continue to improve.

Stopping these trends, or working around them, either through legal or technical means will become more difficult and costly, even when a technical solution is possible. Many of today's cybersecurity problems will be solved a decade from now. As the government and industry meet these compelling demands, both the user environment and the problem set will change radically.

At the same time, these are challenging prospects to the needs of the Intelligence Community and law-enforcement authorities. There is already a dynamic tension between "solutions" to the cybersecurity problem that deny access to data to all but the user and any intended recipient, increased use of encryption, and technical means to work around these solutions. The needs and desires of the Intelligence and law-enforcement communities, however, are not going to prevent the world from "going dark" in many respects, and they may in fact need to look to other means for solving their legitimate mandates. Here there are several open questions to which there are currently no perfect answers.

2. Demand Where Users are No Longer in Control

The transition from the original ARPAnet to the public Internet after 1989 created a new world with many unanticipated consequences. Along with network technology and low cost hardware, other technologies and revolutionary software caused cyberspace to evolve in a way never anticipated—at DARPA or anywhere else. Local and wide-area networks quickly spread through the government, commercial enterprises and educational institutions. Other technologies enabled remote access for users while commercial service providers emerged to meet a rapidly expanding user base.

At the same time, development of the "web" and browser software enabled easy access to rapidly growing net content and applications. Growth of cyberspace during this initial decade of the 1990s was exponential. These were the "Wild West" days of the Internet, and just as there was very little law in the Wild West, there was very little security in cyberspace. In many ways, the 1990s represented a lost decade for cybersecurity as the net rapidly expanded and few programs existed to develop needed security or modernize the vulnerable fundamental net protocols.[16]

The Analog World—Users in Control of Their Data: Until the Internet and digital communications became ubiquitous, almost all files, communications, and data were created in analog form, which could be physically secured.[17] Communications represented a somewhat different problem, but in the analog world telephone calls were not widely recorded and the data did not exist on service providers' servers. Telegrams and faxes were used but did not create permanent digital residue. Today, almost every device is digital and when they are connected to the net, they are all highly vulnerable.

For "data at rest" in the analog world—largely paper files—security and privacy were a physical matter where sensitive materials and data were controlled. Governments

[16] Unfortunately, the Internet continues to operate on network protocols designed decades ago and never intended for the demands of the current era. Solving this fundamental technology problem remains an important challenge. Most experts agree that the current protocols (iPV4 and iPV6) are inadequate.

[17] For generations users invested in physical security systems such as safes, locks, and keys, etc., to protect their secrets and privacy. One extreme option was to rent a safe deposit box at a bank, which was certainly secure, but came with some amount of inconvenience.

kept classified materials in safes and secure facilities.[18] The commercial and private world employed various levels of physical security, although few outside finance or government contracting went to the kind of expense the government paid to protect its sensitive materials. The real need to encrypt was minimal.

The matter of "data in transit" presented different problems. Analog mail services have existed for centuries and the risk of interception along the route has always been an issue.[19] For some government and other communications, manual and machine encryption systems have been employed for centuries, but generally for only a small fraction of communications.[20] As electronic communications came into use, security and privacy issues became more serious, but with few cost-effective solutions available. Analog voice, as well as telegraph and fax messages, could be intercepted and recorded, but cryptographic systems available at the time were all electromechanical, costly, and mostly did not work particularly well. Apart from the government, other users were largely uninterested, and most certainly not willing to bear the costs involved.[21]

The Digital World—Users Are No Longer in Control of Their Data: Transitioning to the digital world has resulted in the disappearance of physical media of all kinds and in a situation where data and files are created in digital form and reside on any number of devices and computer systems in an unencrypted form. The new digital world is also one

[18] The government used, and continues to use, "SCIFs," or sensitive compartmented information facilities, for highly classified data. For many years, computers, copiers and fax machines in such facilities were either banned or tightly controlled.

[19] Intelligence services and law enforcement agencies have long engaged in mail opening operations, both legal and illegal. Users were often aware of the problem, but few were willing to incur the bother to avoid it. Disclosure of an illegal CIA mail opening operation during the Cold War was the subject of a major investigation later disclosed in the 1973 *Family Jewels* report declassified in 2007. Originally operating under the codename SRPOINTER the CIA program intercepted mail destined for the Soviet Union and China from 1952 until 1973 at U.S. postal facilities in New York and Los Angeles.

[20] Ancient history in this area can be found in David Kahn, *The Codebreakers - The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1967). See also, Oded Goldreich, *Foundations of Cryptography*: (Cambridge University Press, 2004). It is also worth noting that for over a century it has been possible to send unbreakable coded messages using a "one time pad," which is a method that is exceedingly inconvenient and useful only for very short messages. See, Frank Miller, *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. (C.M. Cornwell, 1882), and Steven Bellovin, "Frank Miller: Inventor of the One-Time Pad." *Cryptologia* 35 (3): 203–222 (2011).

[21] For required government users, the NSA developed communications systems that were highly secure, but costly and cumbersome. The most serious technical issue of this time was the analog-to-digital conversion, which was the largest element of the system and also costly.

which has seen the merger of information processing and communications. Distinctions between "data at rest" and "data in transit" are not what they were in the analog world as digital data in any location or in a state of transmission have become highly vulnerable.

The most significant aspect of this transition is that users are no longer in control of their own data—locking it up as paper files is no longer a viable option in most cases. Increasingly all interactions with the commercial, legal, financial, medical and personal domains have become interactive ones employing computers and other devices that are part of the connected world. The demand for easy access to data from anywhere has produced extreme vulnerability and access by unauthorized users. Financial and health records, just to take two examples, are all online, and the subjects of the information have virtually no control over the security of their data. Communications almost entirely involves digital telephony, e-mail, web interfaces, file transfers, and text messages.[22] Another troublesome feature of this new world is that in many cases users have little say over what those who hold their data can do with it, as evidenced by the many data breaches seen on a daily basis.

Given this radical paradigm change, it is not surprising that the nature of user demand for security and privacy would change as well. Whereas users could previously provide for their own security and privacy, they cannot do so in the new digital world without the assistance of the commercial suppliers of their communications and related information technology services. Virtually all suppliers have thus far failed miserably in providing anything approaching an acceptable level of security for their customers. Stories of hacks, break-ins, and data theft appear daily in the media.

What Does "Going Dark" Really Entail? As virtually all data and communications now originate in digital form, securing it consists of encrypting then either creating it on a device, or transmitting it through some application. In either case the device or applications uses an encryption algorithm to scramble the digits so that only the user or an intended recipient holding the "key" to the particular file can access the data. A debate now centers on whether commercial firms have access to the keys or can otherwise access user data on behalf of intelligence services and law enforcement authorities. Commercial products and

[22] In the area of telephony, the world has moved increasingly toward mobile systems, while even landlines have moved to VOIP (voice-over-Internet-protocol) systems.

applications increasingly have embedded encryption with only the users holding the keys, and commercial Internet suppliers are unable to offer access to the NSA or anybody else.[23]

In response to greater user demand, common applications will encrypt files as they are created and stored on devices and servers. Encryption algorithms will become part of the user applications and operating systems, much the way a secure protocol has become part of web operations in recent years.

Data Encryption and iPhone Security: Another ongoing debate often referred to as "FBI v. Apple" has now become part of the larger discussion over encryption, particularly since the litigation surrounding efforts to "unlock" an iPhone in the possession of a terrorist in San Bernardino, California.[24] The issue here is one involving a security feature in the iPhone operating system that enables users to "lock" the device so that the data resident on the iPhone can only be accessed by entering the user's passcode. However, not all of the data on the iPhone itself has been encrypted, and once the iPhone is unlocked the FBI can presumably access all data on the device.[25] New releases of the iPhone operating system as well as the introduction of specialized chips for a secure enclave have now made access to new iPhones essentially impossible without the proper passcode.

[23] A release of WhatsApp Messenger, for example, offers users of this (free) application the ability to send encrypted text messages. Text messages are automatically end-to-end encrypted. See: https://www.whatsapp.com/security.

[24] In recent months, there has been extensive publicity over federal legal proceedings in relation to efforts by the FBI to force Apple to created software that would enable the unlocking of an iPhone that was in the possession of a terrorist responsible for the attack in San Bernardino, California. See, for example, Jonathan Zdziarski, "Apple, FBI, and the Burden of Forensic Methodology," (February 18, 2016). Ultimately the FBI was able to "unlock" this iPhone with the help of software from a third party vendor and asked the court to vacate the order. See also, Kim Zetter, "How the Feds Could Get Into iPhones Without Apple's Help," *Wired* (March 2, 2016). While the FBI was ultimately able to access the iPhone in this particular case with the assistance of the outside vendor, the most recent releases of the iPhone operating system (iOS) would render this type of access impossible. It is unlikely that the Government could force Apple to configure new releases of the iOS to enable access in the future.

[25] Apple has previously provided extensive assistance to the FBI and presumably the NSA in a large number of cases where they were able to access both iPhones and unencrypted data on the iCloud.

3. Cybersecurity as a Growing Problem

There is no shortage of studies about the growing problems of cybersecurity as the Internet developed.[26] During this period of explosive growth, entities of all kinds as well as several billion individual users managed to get connected to the net. In addition to hard-wired connections, access became possible through dial-in connections and later a variety of both wired and RF systems. Data stored on computers and personal devices became accessible via the net at far lower costs and with far greater bandwidth.[27] Net access today is largely worldwide and in many cases free.

During this period the nature of data itself was transformed. As the era of "Big Data" evolved, the world moved from an analog to an almost entirely digital one, where physical media of all kinds began to rapidly disappear and digital files on net-based systems became the norm. Records and documents of all kinds came to reside on connected servers. At the same time, the rise of social media added an entirely new dimension to modern life and cyberspace. For its part, the Government joined the stampede into the Internet era with a rapid proliferation of internal networks all connected to the Internet.[28]

[26] See, for example, Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Center for New American Security, 2015); Abraham R. Wagner, *Cybersecurity, Cryptology, and Privacy in Historical Context: The Challenge of New Technologies and Media*, Paper Presented to National Security Agency Cryptologic Symposium (October 2013); Abraham R. Wagner, "Security, Privacy and Technology Development: The Impact on National Security," TEXAS A&M LAW REVIEW (2015); Kerry L. Childe, *Cybersecurity and Privacy: Three Federal Proposals*; Abraham R. Wagner, *Cybersecurity and Privacy: The Challenge of Big Data*, Paper Presented to the Office of Technology Assessment (Executive Office of the President), Big Data Study (March 2014); and Department of Defense, *DoD Cyber Strategy* (April 2015); Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013).

[27] Indeed, as any visitor to Starbucks or most airports can testify, free Internet access via Wi-Fi is readily available.

[28] Initially the Government resisted connecting any computer with classified data to any network, but this approach did not last long. As many of the recent disclosures reveal, classified Government networks with classified data are connected using Internet technology, but are well-protected by high grade cryptographic systems and not susceptible to hacking. Removal of classified data by Edward Snowden and others are cases of espionage by cleared personnel with access to computers rather than cybersecurity problems *per*

In this dynamic environment, users had expectations with respect to privacy and security that changed markedly as they moved into the digital world, and the media made them increasingly aware of the risks and consequences of having their personal information susceptible to hacking and theft. At the same time, it is unclear that users understand what they are really giving up in many cases. They may be increasingly concerned about the lack of security and privacy, but may be largely unaware of what companies are doing with their data, often because they are getting free service from the provider. The legal regime has been at least a generation behind these technological developments, and has provided largely inadequate protections for users.[29]

Possibly the most important concern is that technological developments needed to provide the required level of cybersecurity did not take place during the two decades following the transition to the commercial Internet. The net continues to operate on a set of protocols that are best described as "antique," and related software and other essential software components still contain major vulnerabilities. In large measure cybersecurity continues to be composed of patches, fixes and "band aids" that fail to provide the type of security needed in the current era, and there is no obvious alternative in sight.[30] Nonetheless, it is reasonable to question whether a major overhaul of the operating protocols will provide the needed solution, or whether there is any other realistic alternative to endless patches.

At present the detection of some "hacks," such as zero-day exploits, using manual methods takes on average over 300 days, which is unacceptable. As the 2016 DARPA Cyber Grand Challenge shows, however, the potential exists for greatly improving the process by utilizing supercomputers and advanced software to identify malware, develop

se. The Government does, however, rely almost entirely on the commercial Internet infrastructure for data transmission and is therefore vulnerable to disruption of service and physical attacks.

[29] At present concerns over commercial exploitation, use and misuse of private data are far greater in Europe than in the U.S., with several new laws and court cases in several nations. Unlike the U.S., Europeans seem less concerned about government surveillance programs, which remain the principal focus of civil liberties organizations in the U.S.

[30] For its part even DARPA never had the top level direction since 1990 to undertake the types of programmatic solutions needed or had adequate resources to provide the types of fixes needed. Within the limits of available funding, DARPA continues various cybersecurity programs, as does the Department of Homeland Security (DHS). Most recently DARPA initiated the BRANDEIS program destined to provide a highly innovative approach to individual privacy utilizing some specialized encryption techniques.

"patches" in real time, and avoid system failures.[31] At this stage, whether this type of technology could be developed to a point where it could be operationally deployed remains an open question.

The obvious question is why did the government fail to see this problem and do something more about it? The country did see this, several times, but failed to act effectively. President Clinton recognized the problem and initiated a study of the problem under PPD/NSC-63, and in 1998 set forth the clear intent of the government:[32]

> It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

The Obama Administration similarly recognized that the problem had not been solved, and coming into the era of "Big Data" has made finding a solution more urgent and critical. In PPD-21 President Obama echoed what President Clinton said before:

> The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being. . . Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.[33]

---

[31] Here the DARPA Cyber Grand Challenge demonstrated the ability of supercomputers programmed to detect and "patch" specific malware inserted into the system in real-time. See here: https://cgc.darpa.mil/. This was an initial proof-of-concept demonstration that needs to be further developed for a broad class of exploits in the future.

[32] Presidential Decision Directive/NSC-63, *National Infrastructure Protection*. May 1998. At the time the estimated the cost of achieving this goal was $1.45B which was not included in any federal budget. Further this directive set forth a goal of achieving the needed level of cybersecurity within five years (i.e. by 2003) along with some specific assignments and objectives. It failed, however, to assign actual responsibility for achieving this goal to any agency capable of achieving it or the funds required to develop the technology needed to reach this goal.

[33] Presidential Policy Directive/PPD-21. *Critical Infrastructure Security and Resilience* (February 12, 2013). This directive makes no mention of either the Department of Defense or DARPA. PPD-21 assigns the responsibility for achieving this goal to the Department of Homeland Security (DHS), which has its

For over two decades now, the White House under both political parties has demonstrated an appreciation of the cybersecurity problem and its critical relationship to both national security and the economic well-being of the nation. However, it has thus far failed in either assigning the problem to any federal agency capable of solving it, or even proposing a funded federal program to support a solution. Many of those in government thought this was a problem that would be "solved" by the commercial sector. It was and is not; it is a "public goods" problem that requires programmatic solution by the government.[34]

Can the Cybersecurity Problem Be Solved? This larger question actually comes down to the specific issues of what exactly is the cybersecurity problem; what would a "solution" actually look like; and, what is the set of technical, legal and economic impediments to solving it? A related question of considerable importance is whether a solution may have unintended consequences that pose problems for critical national security and law enforcement functions.

Most technologists agree that the full range of cybersecurity problems cannot be completely "solved" and that there will always be vulnerabilities, particularly in software where new exploits can be developed.[35] It is most likely the case that while all software contains defects which can be exploited, and it may always be possible to develop new exploits to attack these defects, the cost and difficulty of doing so are also likely to increase

---

own Science & Technology Directorate, but still lacks a serious capability to implement an effective solution, and provides no specific funding to achieve it. It also assigns part of the responsibility to the National Institute of Standards and Technology (NIST) which similarly lacks the programmatic infrastructure and funding needed. Similarly, Presidential Policy Directive/PPD-41. *U.S. Cyber Incident Coordination* (July 27, 2016) assigns responsibility to the DHS and the Director of National Intelligence (DNI) with no mention of the Defense Department. Another Obama administration achievement in this area worthy of note is the so-called "Big Data Study" undertaken under the auspices of the White House Office of Science and Technology Policy (OSTP). This study solicited inputs from a wide range of contributors and offers a wide-ranging view of the "big data" problems. While it was a balanced and well-reasoned analysis it too had no programmatic impact on any of the problems discussed. See, *Report to the President: Big Data and Privacy: A Technological Perspective* (May 2014).

[34] See Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, Harvard University Press, 1971).

[35] This state of affairs also makes a compelling argument for an ongoing analytic, research and development process involving both government and the commercial sector to deal with new threats and exploits as they are detected. What exists at present is grossly inadequate, in terms of organization as well as management and funding.

significantly. The user rather than the software is often the weakest link in current cybersecurity.

While avoiding any claim that a complete solution to the cybersecurity problem is achievable, several developments argue strongly that some effective solutions to the most glaring aspects of the current problem are entirely feasible. First, all devices now contain increasingly powerful processors that can implement sophisticated software. There has never been a legal limit on Moore's law, although most agree that the increases in processing power described by Moore are no longer on the path that has prevailed for so long. Second, since high-grade encryption is fundamental to most all aspects of the government cannot use previously used controls on technology that limited its use but also made it more vulnerable and has been forced to abandon the controls previously employed to control this technology and limit its use in terms of key lengths and other criteria which made it vulnerable.

What Would a Solution Look Like? Grappling with this problem is akin to the proverbial blind men trying to describe an elephant by feel, but probably the best way to look at it is in terms of protecting data—including data "at rest" on devices and systems of all kinds, and data "in transit" over the Internet.

Data at Rest. In the current era of "big data," physical media of all kinds is rapidly disappearing and data of every type imaginable resides on a potpourri of electronic devices.[36] Until recently the vast majority of all of these digital files resided on net-connected devices and servers in non-encrypted form for reasons that are not entirely clear. Data access and system maintenance were also performed by software that contained significant vulnerabilities that have repeatedly been exploited. Consider a few recent and illustrative examples:

- ***The Sony Hack:*** A cyberattack on Sony Pictures Entertainment by a group calling themselves "The Guardians of Peace" resulted in a canceled movie release, leaked personal information, and apologies from Hollywood executives caught in embarrassing email conversations.

[36] Evidence of this phenomenon is everywhere. Many newspapers now exist only in digital form; all filings to the federal courts must be as PDF files—not paper; and there is the memorable scene in the film *Social Network* where the statement was made "try and find a record store." Photography utilizing film has become an historic artifact or specialized art form, while most images are now taken in digital form with smartphones or digital cameras.

- ***The OPM Hack:*** A large-scale cyberattack on the federal Office of Personnel Management (OPM) resulted in a large number of personnel files and security clearance data that were stored on old "legacy" computers with grossly inadequate security protection being stolen or compromised.
- ***Explicit Celebrity Images:*** Personal photographs of several celebrities containing sexually explicit images not intended for public distribution were stolen from a cloud server by hackers without permission and subsequently made publicly available on another website.
- ***Hillary Clinton and her Private Server:*** During her tenure as Secretary of State, Hillary Clinton used a personal server for all e-mails including thousands of messages related to her official duties which security experts see as being at least vulnerable to hacking.[37]
- ***Commercial E-Mail Accounts of Key Public Figures:*** The commercial AOL accounts of former CIA Director Brennan and former Secretary of State Colin Powell were hacked, as well as the Gmail account of former White House Chief of Staff John Podesta and various e-mails and personal data were apparently taken. In the case of Secretary Powell and Mr. Podesta, some of the e-mails were released on a suspect website in an apparent effort to influence the 2016 Presidential election.
- ***Russian Hack of the DNC and Campaign Personnel:*** According to various Intelligence Community reports, the computer network of the Democratic National Committee (DNC) was hacked by Russians who reportedly gained access to the entire database of opposition research on presidential candidate Donald Trump and were also able to read all e-mail and chat traffic. Additional hacks of e-mails reportedly belonging to several Democratic campaign officials were made public by the WikiLeaks website in what some believe to be a Russian attempt to influence the 2016 U.S. Presidential election.[38]

[37] Some analysts contend that this private system was likely to have been hacked by several foreign intelligence services and at least one individual hacker has already testified to having done so. In all fairness, it is the case that countless numbers of Government personnel maintain personal e-mail accounts with commercial services and often use these accounts for communications related to Government business. Consistent policy and enforcement remains an issue for the Government.

[38] Several accounts attribute the hacks to two Russian hacking organizations, known as "Cozy Bear" and "Fancy Bear." Each had a relationship to an official Russian intelligence service—the FSB and the GRU.

Each of these examples involves user data, both individual and enterprise, which existed on a server in an unencrypted form and was not shared with other parties voluntarily or with knowledge. It is also clear that these users had a substantial desire for privacy and security but were not fully aware of the risks and vulnerabilities when entrusting their private data to their respective systems.

Some authorities have used the analogy where customers or "users" entrust their valuables to a bank, which utilizes various security procedures such as safe deposit boxes, a vault and an armed guard at the front to thwart theft. Here the bank can be held liable for losses where thieves cause this trust to be violated. In cyberspace, however, such an analogy often fails where the service provider may be outside U.S. jurisdiction or otherwise unable to provide the requisite security or pay when the trust is breached. Effective security solutions must be provided at the user level, not at the level of the service provider who cannot always be held accountable. In the interim, however, regulating providers offering secure and trustworthy cloud storage may be a reasonable approach.

As the examples given above clearly illustrated, both government and commercial service providers failed to adopt cryptographic security measures for the data entrusted to them when they could easily have done so.[39] It remains the case that massive amounts of data continue to reside on servers in an unencrypted form when secure and viable alternatives are available. At present a new era in user demands and expectations of privacy and security may ultimately force a long-needed change.

On the other hand, it is important to recognize that encrypted information on servers does not by itself ensure the security of that information. If legitimate users have access to decrypt the information then either authentic users with malicious intent (Edward Snowden) or illegitimate users who have stolen access credentials, will be able to access the data at least to some extent. For example John Podesta's emails were reportedly accessed not through a software vulnerability, but by a "spearfishing" attack in which he revealed his Gmail password in response to an email masquerading as an urgent request from Google for him to change is password in response to a compromise of his account

Separately evidence suggests that the e-mail accounts of some DNC and campaign personnel on commercial services (like Gmail and AOL) were also the subject of hacking and subsequently made available on the WikiLeaks website.

[39] In the aftermath of the most recent OPM scandal, that agency claimed that it would not have been possible to do so with the old "legacy" systems they had. A subsequent analysis of the substantial funding available to OPM to solve the problem renders this excuse particularly lame.

security. Although software limiting access out of established patterns and biometric access control techniques can limit such breaches, we should not pretend that encryption and related software fixes will produce complete cybersecurity.

The Role of Encryption and Differential Privacy: The various examples listed above have in common the fact that the personal, and in some cases classified, data resided on systems and servers in an unencrypted form which could be read or viewed by anybody with access to the system. Here the critical question is why? The classified data on U.S. Government systems is protected (encrypted) by NSA systems, and relatively effective cryptographic software and algorithms have been commercially available for years.[40] It is important to note that only a fraction of U.S. Government communications are in fact protected and at least some of the unclassified Government e-mail is still outsourced to Google (Gmail). Fortunately, classified Government e-mail systems are configured in a way that data on these protected systems cannot be forwarded to an unclassified system.[41]

The answer lies, in part, with the commercial service providers and software firms that simply failed to implement fairly simple technical solutions for reasons of perceived cost, lack of user demand, or inertia.[42] Furthermore, U.S. policy was long driven by the desire to control encryption technology, including cryptographic and cryptanalysis systems, for national security purposes. The multiple objectives were to: (1) protect sensitive U.S. communications; (2) deny adversaries cryptanalytic capabilities; and (3) enable U.S. cryptanalysis of foreign systems by denying adversaries better cryptographic capabilities. For decades these technologies included electromechanical systems,

[40] The complete name of that agency is NSA/CSS, where the "CSS" stands for Central Security Service. By Presidential Directive (1952) CSS provides cryptographic services for all U.S. Government requirements, including hardware, software and support services. Largely unknown, CSS ranks as one of the best run elements of the U.S. Government.

[41] As recent espionage cases show, it has unfortunately been the case that materials from classified systems could be removed using a USB "flash" drive and later transferred to another (non-secure) system. This appears to have been the case with Edward Snowden who removed a large volume of classified materials from a computer in Hawaii connected to a Top Secret network.

[42] An additional explanation might be that they were under some pressure—either real or imagined, that the Government did not want them to encrypt data in their custody.

specialized chips, and software and encryption algorithms.[43] In the beginning private user needs for secure systems were not a significant issue.

Government policy has radically changed for legal and technical reasons. In the legal arena, the federal appellate court in 1999 largely stopped the Government's longstanding efforts to limit and control university research in cryptography.[44] More recently, however, the problem has become moot as relatively high-grade encryption algorithms have become available worldwide, both on the Internet and from commercial suppliers over which the U.S. Government has no control.

Where commercial systems were either implemented (*e.g.*, PGP, RSA, etc.) or proposed, the Government sought various forms of control and access, either by limiting key lengths or proposing nonsensical "key escrow" systems such as the Clipper Chip. Less well-known were Government efforts to install "back doors" in software which would assure ongoing access to encrypted data. Ultimately all such efforts failed for various reasons.

The discussion above largely relates to what may be termed "simple privacy"—*i.e.*, the desire for users to have their data held in a private and secure manner. In the modern world, however, users have a need to share private or sensitive information with others, and the service provider or a "trusted party" dataset (*e.g.,* medical records, voter registration information, e-mail usage, etc.) with the goal of providing global, statistical information about the data publicly available, while preserving the privacy of the users whose information the data set contains. Here the concept of indistinguishability, later

[43] See Kahn, *The Codebreakers, op. cit.* and Goldreich, *Foundations of Cryptography, op. cit.* More recently (December 2013) the list of controlled technologies was amended to include surveillance systems for the first time linking exports of Western surveillance technologies to human rights abuses in several countries. The list of "cybersecurity" items, now including traditional "information security" functionality" such as encryption and cryptanalysis, as well as adding a new category termed "intrusion software" significantly expanding the concept.

[44] The critical case here is *Bernstein v. Department of Justice*, 176 F.3d 1132 (9th Cir. 1999). This was actually a series of cases in the Ninth Circuit Court of Appeals and never reached the Supreme Court. Here Bernstein won against Government efforts to control the dissemination of his unclassified research in cryptography, which sought to do so on "national security" grounds. A more extensive discussion can be found in Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (New York: Viking Penguin, 2001).

termed differential privacy, formalizes the notion of "privacy" in such shared or statistical databases.[45]

The fundamental objective in these types of situations then becomes one of having the user or creator of the private data in control of their data at all times, as well as having the ability to securely "share" the data with other trusted users when needed. This requires a different and somewhat more complex set of cryptographic techniques currently under development.

[45] Such a system is called a statistical database. The notion of indistinguishability, later termed "Differential Privacy" formalizes the notion of "privacy" in statistical databases. See, for example, A. Ghosh, T. Roughgarden, and M. Sundararajan. "Universally utility-maximizing privacy mechanisms" in *Proceedings of the 41st annual ACM Symposium on Theory of Computing*, (New York: ACM, 2009); Konstantinos Chatzikokolakis, *et al* "Broadening the scope of Differential Privacy Using Metrics" in *Privacy Enhancing Technologies*, (Berlin-Heidelberg: Springer, 2013). See also, Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel "Unique in the Crowd: The privacy bounds of human mobility." *Nature* (March 25, 2013).

4. Commercial Encryption—Why it Failed Before

Providing privacy and security through encryption is not a new concept, and history is replete with attempts by commercial firms to provide such solutions. Most of these systems were commercial failures as there was simply no compelling user demand, and they were costly electromechanical devices for which there was a very limited market.[46]

As the world moved away from stand-alone electromechanical systems to specialized chips, even software solutions created by commercial service providers and software firms failed to implement fairly simple technical solutions for reasons of perceived cost, lack of user demand, or inertia.[47] It is also the case that the government was averse to such solutions which involved high grade encryption that could not be readily accessed, and in the fact for many years sought to control the development and implementation of cryptographic software as a matter of national security policy. This was driven by the desire to control encryption technology, including cryptographic and cryptanalysis systems, for national security purposes. Even private, unclassified university research was subject to strict governmental control and the publication of results was restricted.

Aside from government efforts to control commercial encryption over the years, virtually all efforts to market commercial encryption systems have failed for at least one of three fundamental reasons: (1) it cost the user money; (2) it imposed inconvenience on the user (*i.e.*, it required the user to act in some way); or (3) it degraded quality in any way.[48] For decades all commercial encryption systems, whether complex electromechanical systems or electronic specialized chip systems, violated one or more of these conditions.

[46] The demand for commercial cryptographic systems at the time came largely from foreign governments who desired to secure their communications and did not have a domestic industry capable of producing such devices.

[47] An additional explanation might be that they were under some pressure—either real or imagined, that the government did not want them to encrypt data in their custody.

[48] One classic example is the German *Enigma* machine which was developed just prior to World War II as a commercial product. It was thoroughly rejected by potential commercial customers and its inventor went bankrupt, only to be taken over by the Nazi Government and utilized as a military system. See Tom Perera, *The Story of the ENIGMA: History, Technology and Deciphering, (2nd Edition),* (Artifax Books, 2004) and F.W. Winterbotham, *The Ultra Secret.* (London: Weidenfeld & Nicolson, 1999).

Studies undertaken during the 1990s predicted that commercial encryption would become far more pervasive and an integral part of both operating systems and application software in a few years. For the most part, these predictions failed to materialize as expected in the anticipated time frame.[49]

By 1990 costly electromechanical encryption had given way to specialized computer chips, such as the proposed "Clipper Chip" in cell phones.[50] At the time several organizations challenged the Clipper Chip proposal, saying that it would have the effect of subjecting citizens to increased and possibly illegal government surveillance.[51] The strength of the Clipper Chip's encryption could not be evaluated by the public as its design was classified. Further, while American companies could be forced to use the Clipper Chip in their products, foreign companies could not. This meant that phones with stronger data encryption could be manufactured abroad and made available in the U.S., largely negating the point of the entire concept.

The idea of specialized encryption chips was short-lived, and gave way to devices with increasingly powerful general-purpose processors that can run any one of the strong cryptographic software packages that are becoming available, such as Nautilus, PGP and PGPfone. As time moved on, relatively strong cryptography was becoming freely available on the Internet, and the U.S. Government was unable to stop its use.

[49] Microsoft, for example, could easily have incorporated cryptographic algorithms into both their operating systems and application software, at no marginal cost to users, and simply did not do so. An alternate example is the introduction of the secure hypertext transfer protocol (://https) which enables relatively secure credit card purchases, at no additional cost or inconvenience to users: online shoppers do not have to "do" anything extra, it simply works.

[50] The Clipper Chip was developed and promoted by NSA and the FBI as an encryption device, with a built-in "backdoor," intended to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct. The Clipper Chip used NSA's Skipjack data encryption algorithm to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers. Invented by NSA, Skipjack was initially classified, which prevented it from being subjected to peer review by the encryption research community.

[51] The two leading groups opposing the Clipper Chip were the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF). In addition, then-Senators John Ashcroft and John Kerry opposed the Clipper Chip proposal, arguing in favor of the individual's right to encrypt messages and export encryption software.

5. Constraints on Encryption

With respect to government policy, the world has radically changed for legal and technical reasons. Within the government, cryptographic developments were all originally undertaken at the NSA, where classification and strict security were rigidly enforced. The government also exercised control over unclassified university research and the types of systems that could be sold commercially. In recent years, however, both the federal courts and technical realities have upset this well-ordered universe.

The Collapse of Legal Controls on Encryption—Cryptographic Research: Up until the 1970s, research into cryptography was primarily the domain of the government, and in particular the National Security Agency (NSA).[52] The government had been interested in cryptography since at least World War I and continued to invest heavily in the development of cryptographic systems throughout the early years of the Cold War.[53] In the mid-1970s, NSA played a critical role in developing the first Data Encryption Standard (DES) alongside IBM.

As interest in cryptography grew along with the development of modern computers the NSA slowly lost control. Despite its efforts, in 1977 the NSA agreed that it did not have complete control over federal cryptography research, and the National Science Foundation began awarding grants to study encryption.[54] The NSA continued to fight for several years. This included vigorous attempts to classify cryptography developed by non-government researchers and, in 1982, the elimination of the Commerce Department's civilian computer security program.[55]

Nevertheless, public research into encryption continued. In 1976, Stanford University researchers published a paper on "public key cryptography," and by 1977, three MIT professors had invented the first public-key encryption system, RSA. The government then started to employ the International Traffic in Arms Regulations (ITAR) and the Arms

[52] *Cryptography's Role in Securing the Information Society,* (Nat'l Academies Press, 2016).

[53] Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 IND. L.J. 101, 109 (2015).

[54] David Banisar, *Stopping Science: The Case of Cryptography*, 9 HEALTH MATRIX 253, 256 (1999).

[55] *Id.*

Export Control Act (AECA) to try and control dissemination of information regarding cryptography. This, alongside expanded NSA power to control encryption under President Reagan's National Security Decision Directive, NSDD-145, effectively expanded government control over cryptographic research.[56]

These long standing and largely successful efforts by the government to limit and control university research in cryptography were largely stopped by the federal courts in 1999. The critical case was *Bernstein v. Department of Justice*.[57] It was actually a series of cases in the Ninth Circuit Court of Appeals that never reached the Supreme Court. Bernstein, a professor of mathematics, had developed an encryption algorithm. The State Department prohibited Bernstein from publishing his work, stating that he needed an export license as required by ITAR. Bernstein challenged the government's efforts to control the dissemination of his unclassified research in cryptography on "national security" grounds.[58]

The Ninth Circuit struck down the regulations on Bernstein's publication of his research: "because the prepublication licensing regime challenged here applie[d] directly to scientific expression, vest[ed] boundless discretion in government officials, and lack[ed] adequate procedural safeguards, it constitute[d] an impermissible prior restraint on speech."[59] One year later, the Sixth Circuit likewise concluded that "computer source code . . . is protected by the First Amendment."[60]

Following *Bernstein* and *Junger*, public research in cryptography has not faced vigorous federal regulation and control like it once did. More recently, the problem has largely become moot because high-grade encryption algorithms are available worldwide, from both the Internet and commercial suppliers over which the U.S. Government has no control.

Privacy and Security Issues: Understanding solutions to the cybersecurity problem requires some understanding of the closely related concept of "privacy" and how it has

---

[56] *National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive, NSDD-145 (September 18, 1984).

[57] 176 F.3d 1132 (9th Cir. 1999).

[58] A more extensive discussion can be found in Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (New York: Viking Penguin, 2001).

[59] *Bernstein*, 176 F.3d at 1145.

[60] *Junger v. Daley*, 209 F.3d 481, 485 (2000).

evolved.[61] Over time, the concept of privacy has changed significantly, not only as a result of the legal regime but also because of supporting technologies and what users have come to expect. The Founding Fathers saw privacy as essential to a free society, and embodied this concept in the Fourth Amendment to the Constitution. Their view of privacy, however, was formed in an era that predated electronic communication by half a century and they largely defined privacy in terms of the sanctity of the home as a private place. The subject of privacy in electronic communications did not even come before the Supreme Court until 1928 when a majority of the Court held that the Fourth Amendment did not apply to such communications.[62]

Almost 40 years later, in 1967, the landmark Supreme Court decision in *Katz v. United States* altered the concept of privacy in several respects. First, the Court reversed *Olmstead*, finding instead that the Fourth Amendment privacy guarantees did in fact apply to electronic communications.[63] But the Court went further by holding that privacy rights attached to persons, not simply places. This was a substantial shift, since the Court's analysis until 1967 revolved around whether the area intruded upon was constitutionally protected as "private," regardless of how it was used.[64] This dramatic expansion, however, did not mean that the right to privacy was absolute. Instead, Justice Harlan laid out a two-prong test, later adopted by the entire Court: the right to privacy attached where (1) people had a subjective expectation of privacy, and (2) which society recognized as reasonable.[65]

Katz came at a time when the world was far simpler technologically: virtually all users were individuals; cyberspace was a decade away; databases were not yet on networked systems; and social media was not yet on the horizon. For all its flexibility and longevity, the *Katz* test has not perfectly adapted to the modern world. The *Katz* decision,

---

[61] Abraham Wagner, *Cybersecurity and Privacy: The Challenge of Big Data,* Paper Presented to the Office of Technology Assessment (Executive Office of the President), Big Data Study (March 2014).

[62] *Olmstead v. United States*, 277 U.S. 438 (1928). Majority opinion by Chief Justice Taft. A dissenting opinion by Justice Brandeis found otherwise, but was not the law until the *Katz* decision in 1967.

[63] *Katz v. United States*, 389 U.S. 347 (1967).

[64] Recently, the Court announced that *Katz* did not displace the old analysis entirely. This means that trespass into a constitutionally protected area is *per se* a violation of privacy. *See United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945 (2012).

[65] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

which considered whether Mr. Katz's conversation with his bookie inside of a telephone booth was private, presumed that privacy is a binary concept: information either is private or it is not. While a telephone call between two individuals may be inherently private, most telephone calls do not involve data stored with a third party. In fact, shortly after *Katz*, the Court recognized that data provided to a third party for business purposes does not receive the same protections.[66] Since the 1960s, available technologies have increasingly enabled not only data storage, but also personal sharing of private data among some set of people that presumably the user wishes to control. The nature and extent of permissible sharing goes to the heart of many current problems.

More specifically, the advent of social media and related applications poses a significant challenge to the more traditional binary concept of private and not-private data. Users store an ever-growing body of data on servers owned by companies like Facebook and Google. However, the users only intend to share information with a limited set of people—or possibly the public at large. While the data is stored on these servers it is accessed by the service provider and used for commercial purposes. Although users ostensibly consent to the terms of service, which permits service providers to access their data, users rarely read these policies all the way. This has caused many to question the voluntariness of the consent given.[67]

Nevertheless, users may expect that these companies will respect their privacy—or at the very least not sell their personal information—while also sharing the same information with other users. Under the old *Katz* test, this information would necessarily be not-private, even though most people would agree that information shared with a select group of people is private. This conundrum gives rise to the possibility of "quasi-private" information: data which the user intends to share with some limited, but possibly not well defined, set of others. This may become a key component of the concept of data sharing as it evolves over time.

Another consideration is a distinction in the type of user: individuals or "enterprise" users, such as government agencies or corporations. Corporations, for example, have large

[66] *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976). While the so-called "Third Party Doctrine" established in *Smith* has been the law, it appears to be rapidly eroding as witnessed in recent battles over surveillance and "metadata." Some legal scholars believe that the Supreme Court will overturn *Smith* in the near future.

[67] *See, e.g.*, Mary G. Leary, *Katz on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 356-361 (2013).

amounts of data involving their business, operations, intellectual property, and other sensitive information which they do not wish to make available or wish to share with only a limited set of external users. To some extent, the legal regime has provided some protection for this type of data through intellectual property law, although such protections are far from adequate or even fully enforceable in the real world.[68] Even though the legal regime has yet to deem this type of data as "private" within the context of the Fourth Amendment, it is abundantly clear that maintaining such data securely and limiting sharing to authorized or agreed upon uses is essential to the economic health of the nation.

The fundamental point here is that as law and technology change, user expectations with respect to privacy and security also change. Both individual and enterprise users are increasingly aware that much of their data is no longer under their personal control, but resident on devices and networked data servers over which they have far less control and confidence. Fueled by endless news reports, as well as lawsuits from the ACLU, the Electronic Frontier Foundation (EFF) and others, users are concerned about hacks, theft, unauthorized access, and other forms of intrusion in their personal lives from not only adversaries but law enforcement and intelligence services who seek to protect them.[69]

These myriad questions have left the legal status of encryption as it relates to privacy somewhat obscure. Numerous commentators have suggested that people who use encryption have an expectation of privacy that society may recognize as reasonable.[70] Others have stated that the way the technology functions means that encryption cannot and

[68] The federal government has been somewhat more successful where classified data is involved through the use of security clearances and secure systems for maintaining classified data. Even so, recent espionage cases such as Snowden and the WikiLeaks cases demonstrate the problems that arise from unauthorized access and unintended sharing. Even government officials have been found to be negligent in handling sensitive classified materials on unsecure computer systems or in using commercial e-mail accounts.

[69] It is worth noting that in Europe the law is evolving quite differently. There, users', courts' and several European parliaments' accept as legitimate the interests of intelligence and law enforcement, but have focused their concerns on commercial surveillance for business exploitation. See here, *Second Legal Challenge Against Privacy Shield* (November 3, 2016), https://epic.org/2016/11/second-legal-challenge-launche.html

[70] See, for example, Wayne R. LaFave, 1 SEARCH & SEIZURE § 2.6(f) (5th ed. 2012) ("It depends on whether you look at how the technology works or social understandings. If you focus on social understandings, the prevailing social understanding today is that using encryption is a good way of making something private."); see also, *United States v. Zhu*, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014) ("Zhu's use of passwords and encryption weighs in favor of finding a reasonable expectation of privacy").

does not create an expectation of privacy.[71] The Supreme Court has, however, repeatedly stated that privacy as defined by the Fourth Amendment relies on social conceptions, not the particular technology at issue.[72] To some extent, law enforcement concerns surrounding encryption recognize that encryption creates an expectation of privacy, just as other private forms of communication.[73] That is why the FBI and other agencies have recognized the need for prior judicial authorization, often in the form of a warrant, to access electronic communications.[74]

The question remains, however, whether quasi-private communications or communications among enterprise users should receive the same level of protection as electronic exchanges between two people. If encryption confers a reasonable expectation of privacy on message because of the social expectation surrounding it, then the question becomes whether communications that are released to a limited set of other people also carry an expectation of privacy and if encryption in any way impacts that determination. Courts and commentators have divided over the former, but, at the very least, encryption enhances the expectation of privacy in all communications, not just those between two individual users.[75]

---

[71] See, Orin Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 505 (2001) ("[E]ncryption cannot create Fourth Amendment protection . . . Once cypertext is in plain view, the communication itself is in plain view for Fourth Amendment purposes. Although the government must unscramble the communication to understand it, the Fourth Amendment cannot regulate the cognitive process by which the government attempts to extract meaning from an encrypted communication in its possession.").

[72] *Cf. Minnesota v. Olson*, 495 U.S. 91, 98 (1990) ("Staying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society."); *Kyllo v. United States*, 533 U.S. 27, 35-36 (2001) (" . . that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

[73] See James Comey, *Encryption Tightrope: Balancing Americans' Security and Privacy*, FBI (Mar. 1, 2016), https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy ("We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology . . . the Constitution demands it.").

[74] *Id.* ("One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence.")

[75] Compare *United States v. Meregildo*, 884 F. Supp. 2d 523 (S.D.N.Y. 2012) ("Postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally

Encryption, then, adds another layer of protection to a communication, not just technically, but also legally. Even if a message is quasi-private, encrypting it imbues it with a greater level of privacy protection, which suggests that law enforcement should go through a more rigorous judicial screening process to access it than if it were actually released to the public. This is not to suggest that encryption creates a total legal privacy shield; law enforcement can still access encrypted data with a warrant and may even be able to compel disclosure of a cryptographic key or passcode, although the latter proposition remains an open question.[76]

Nonetheless, in part because encryption provides this heightened level of privacy and security to electronic communications, the government has sought other ways to regulate cryptographic technologies. Driven by national security concerns, the government has attempted to create a series of frameworks to control both research into and applications of cryptography, but each of these attempts has failed, for a combination of the legal reasons discussed above and for technological reasons that will be discussed below.

Commercial Algorithms and Keys: In the early 1990s several commercial encryption products became available to provide Internet users with some degree of protection, such as PGP (Pretty Good Privacy).[77] Like earlier systems, such as RSA, PGP employs the concept of an asymmetric public-private key cryptosystem. Most experts

protected"); Stephen E. Henderson, *Expectation of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 241 (2012) ("As to friend wall posts, protected tweets, and similarly limited communications, there is a Fourth Amendment expectation of privacy.") *with Reid v. Ingerman Smith LLP*, 2012 WL 6720752 (E.D.N.Y. 2012) (finding that a user has no reasonable expectation of privacy, even if their privacy settings only allow Facebook friends to see their postings).

[76] Compare *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (holding that compelling a defendant to enter an encryption key would not violate the Fifth Amendment privilege against self-incrimination) with *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) (holding that compelling an individual to decrypt a hard drive's contents violated the Fifth Amendment protections against self-incrimination).

[77] Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication and was created by Phil Zimmermann in 1991. PGP and similar software follow the RFC 4880 standard (RFC 4880) for encrypting and decrypting data whereby the message is encrypted using a symmetric encryption algorithm. Each symmetric key is used only once and is also called a session key. The message and its session key are sent to the receiver. The session key must be sent to the receiver so they know how to decrypt the message, but to protect it during transmission, it is encrypted with the receiver's public key. Only the private key belonging to the receiver can decrypt the session key. The idea of an asymmetric public-private key cryptosystem is attributed to Diffie and Hellman, who published the concept in 1976.

agree that indeed, the level of protection afforded by such systems is "pretty good" and even the intelligence services were relatively comfortable with their proliferation and use.[78] While not officially stated, it can be assumed that organizations such as NSA were able to deal effectively with PGP-encrypted files.

Even though PGP and its predecessors were largely free for users, they were not widely used. User demand did not accelerate at the time, and use of PGP software required additional effort and inconvenience, which most users were not willing to undertake. This point cannot be overstated – users simply do not want to deal with encryption that costs anything or requires additional effort.[79]

Conversely, when encryption is made freely available and does not require any action by the user, it can spread rapidly. For example, the HTTPS protocol, which helps protect communications between a user and a particular web service, has become commonplace. HTTPS operates by verifying the identity of a web service for a user through cryptographically signed certificates; it also encrypts communications between the service and the user. Although HTTPS only protects against certain types of intrusions and may have some impact on performance, it has been widely implemented without any required action on the part of the consumer.[80] Even though it does not offer very vigorous protection, it has become the standard for a wide range of online business transactions and even simple web browsing.

Cryptographic Technology and Arms Exports: Despite the *Bernstein* holding, there has been a recent resurgence in attempts to regulate encryption through export controls. Most significantly, the Department of Commerce, Bureau of Industry and Security (BIS), proposed the implementation of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies, which sought to control the export of encryption technology and an expanded list of controlled technologies. These technologies included surveillance systems in response to reports linking exports of

[78] See, for example, Bruce Schneier, *Applied Cryptography*. (New York: Wiley, 1995).

[79] User problems with PGP are well-documented, and for the most part users had difficulty performing even basic tasks such as encrypting and decrypting messages. See Sara Sinclair Brody, *Protecting Data Privacy With User-Friendly Software,* Council on Foreign Relations Cyber Brief (May 2016). See also, Alma Whitten and J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (Carnegie Mellon University, 1998).

[80] World Wide Web Consortium, *Securing the Web* (Jan. 22, 2015), https://www.w3.org/2001/tag/doc/web-https.

Western surveillance technologies to human rights abuses in countries such as Bahrain, the United Arab Emirates, Turkmenistan, and Libya.[81] The proposal raised serious concerns among a variety of groups in the U.S., including government offices, software developers, hackers, lawyers, and civil liberties organizations.

The intent of the 2013 Wassenaar language was to provide legal tools to combat the sale of surveillance software to repressive government regimes. Virtually all experts, however, agreed that this objective would not be achieved. Foreign governments and nefarious groups seeking to obtain such software can obtain it irrespective of export controls implemented by the Wassenaar signatory states. Underlying many of the criticisms of the Wassenaar Arrangement was a fundamental concern: because of how rapidly, frequently, and easily different technologies can be transmitted across the globe, export restrictions are not an effective tool for regulating technology.

In the U.S. and elsewhere such controls began at a time when exports consisted of physical goods that were actually shipped by sea, air or land. Controlling and licensing exports made sense and could be subjected to various controls at physical, geographical boundaries. The evolution of not only the Internet but software as a non-physical "good"

[81] In particular the December 2013 Wassenaar plenary meeting ratified proposals from the UK and France aimed at curbing the transfer of commercial surveillance software products and IP network surveillance systems that are known to have been used by foreign government engaged in repressive activities against their citizenry, contributing to alleged human rights abuses. See, for example, Karen McVeigh, "British Firm Offered Spying Software to Egyptian Regime," *The Guardian* (April 28, 2011), http://www.theguardian.com/technology/2011/apr/28/egyptspyingsoftwaregammafinfisher; Morgan Marquis-Boire and Seth Hardy, "Syrian Activists Targeted with BlackShades Spy Software," *The Citizen Lab Research Brief No. 6* (June 2012), https://citizenlab.org/wpcontent/uploads/2015/03/SyrianActivistsTargetedwithBlackShadesSpySoftware.pdf; Morgan Marquis-Boire, Backdoors are Forever: Hacking Team and the Targeting of Dissent," *The Citizen Lab Research Brief No. 12* (October 2012), https://citizenlab.org/wpcontent/uploads/2015/03/BackdoorsareForeverHackingTeamandtheTargetingofDissent_websitepdf.pdf. Recently published research, however, indicates that such proposed rules may not actually solve the problem. See here, Robert Falcone and Jen Miller-Osborne, "Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists," http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/.

has rendered geography largely irrelevant. Moreover, it is exceedingly difficult to apply export controls to "goods" that do not yet exist, such as software.[82]

One of the most serious unintended consequences of the regime would be the highly adverse impact on the development of essential cybersecurity software. Multinational companies have raised significant concerns about export controls on technology.[83] Cybersecurity companies in particular noted that the nature of modern information security requires them to send technology and information across borders, often at a moment's notice, in order to effectively defend against the wide range of threats.

Despite these criticisms, the U.S. Government has continued to try and impose export controls on encryption.[84] These controls extend to a range of encryption tools and software and are governed by the Export Administration Regulations although these controls are only occasionally enforced.[85] By and large the restrictions have eased, if only because an increasing number of encryption protocols have fallen into the category of "publicly available" software, which is not subject to the same controls that are imposed on other forms of encryption.[86] As encryption technology becomes increasingly popular and readily available, these controls will become even weaker and will no longer provide any meaningful restraint on widespread use of encryption.

In the years ahead, the U.S. will need to come to grips with the fact that this is an area which is beyond its control, and even beyond the control of the forty-one nations that are current signatories to international agreements such as the Wassenaar Arrangement. Cyberspace is "borderless" and legislation by an individual nation, or even a cooperative

---

[82] Cf. *ClearCorrect Operating, LLC v. Int'l Trade Comm'n*, 810 F.3d 1283 (Fed. Cir. 2015) (holding that the term "articles" refers only to material things and cannot be used to apply laws governing unfair trade practices to electronically transmitted digital data).

[83] See *Wassenaar: Cybersecurity and Export Control: Hearing before the Subcomm. on Information Technology of the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (2016).

[84] *See Encryption*, DEP'T OF COMMERCE BUREAU OF IND. AND SEC'Y, https://www.bis.doc.gov/index.php/policy-guidance/encryption.

[85] *Intel Subsidiary Agrees to $750,000 Penalty for Unauthorized Encryption Exports*, BUREAU OF IND. AND SEC'Y (Oct. 8, 2014), http://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/107-about-bis/newsroom/press-releases/press-release-2014/763-intel-subsidiary-agrees-to-750-000-penalty-for-unauthorized-encryption-exports.

[86] United States Eases Export Controls on Certain Encryption Software, GIBSON DUNN (Jan. 19, 2011), http://www.gibsondunn.com/publications/pages/USEasesExportControls-CertainEncryptionSoftware.aspx.

agreement among a group of nations, cannot be effective in controlling the proliferation of these technologies.[87] A few short years ago, the U.S. was still trying to impose criminal penalties on the distribution of encryption software that was at the time freely available on the Internet. The lesson here is that now, and for certain in the years to come, efforts to limit software development and distribution are doomed to fail and may have the unintended consequence of impeding potentially useful software development in the U.S. and elsewhere by restricting development tools essential to security research.

Encryption and the Expectation of Privacy: The availability of practical and low-cost encryption for communications and data raises the issue of whether the use of encryption creates any new or additional expectation of privacy. One could argue that the need to encrypt indicates that the user has no expectation of privacy and must take steps to ensure privacy because the law offers no protection. However, in the current technical environment, the law offers a degree of protection against unlawful intercept by lawful agencies. That legal protection is essentially worthless however, where hackers and foreign intelligence services may be engaged.[88]

The most widely accepted view of *Katz*, generally taken from Justice Harlan's concurring opinion, is that there is actually a two prong test: to receive the legal protections of the Fourth Amendment, first, individuals must have a subjective expectation of privacy, which may be evidenced by their actions, and, second, society must be willing to accept that expectation as "reasonable." In *Katz*, Katz stepped inside of a public phone booth and closed the door behind him in order to communicate with his bookie. The Court concluded that, by entering an area that made it difficult for the public to hear his conversation, Katz was demonstrating his subjective expectation of privacy. Since *Katz* (1967), the courts have generally held that the content of any communication is protected if the communication satisfies the two-prong test in *Katz*.

Therefore, the current need to encrypt follows not from the failure of the courts to recognize an expectation of privacy, but from various third parties that are hacking and stealing personal data. In most cases, third parties—other than law enforcement and intelligence agencies—operate beyond the practical reach of the courts, so users must

[87] See Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006). The situation here is unlike nuclear proliferation, where the key technologies and resources are controlled by a limited number of states that have been relatively effective in limiting proliferation in this area.

[88] *Cf. Katz v. United States*, op. cit.

protect their communications using technical means as opposed to relying on the legal regime. Conversely, even when a user has an expectation of privacy recognized by society as reasonable under *Katz*, law enforcement and intelligence agencies may lawfully access these communications with a warrant.

One way to look at things is that in practical terms, *Katz* was an effort by the ACLU and other civil liberties lawyers to overturn *Olmstead* (1928). While the privacy of telephone communications was not a major concern for millions of phone users, the current situation is different. In the transition from the analog to the digital world users have lost control over their personal data and communications, and given the publicity and leaks surrounding various surveillance programs, security of digital communications has become a huge issue for many— not just the ACLU and EFF. Encryption is an easy and practical technical fix to this large problem that no court could ever fix, especially because the best hackers are beyond U.S. jurisdiction.

Certainly when a user employs encryption, or even uses an application with embedded encryption, there is an expectation that satisfies the first prong of the test in *Katz.* It also can be seen to satisfy the second prong of the *Katz* test as well: modern society recognizes as perfectly reasonable an expectation that personal communications and data can and should be protected from third parties such as hackers, cyber-criminals, and foreign intelligence services with the use of encryption technology.

The most current concerns which are not yet resolved in the courts largely relate to data residing on devices such as "smartphones" which may be encrypted or otherwise locked with a password. Here, the issues are mostly whether users can be compelled to disclose their passwords to law enforcement authorities, and, absent the user, can the device manufacturer or service provider be compelled to "unlock" the device. A related question is whether a firm such as Apple can be compelled to write new software that would enable privacy features to be defeated.[89]

[89] See, for example, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (C.D.C.A.: 16-cm-00010-SP). While this case was dismissed by the Government prior to trial, the excellent briefs by the parties as well as the *Amici Curiae* are highly informative with respect to both the legal and technical issues in this critical area. As the FBI was able to access the iPhone in question with the aid of an outside contractor the issue before this court became moot. As discussed *supra,* the proposed Burr-Feinstein (2016) Senate bill is a legislative attempt to deal with this matter, but suffers from several fatal defects and is unlikely to become law.

6. Encryption Technology—Power and Potential

What is Encryption?: The centerpiece of the entire discussion is encryption, which consists of converting readable "plain text" into "cipher text" or a scrambled form that cannot be read without the requisite software and "key."[90] This process ensures that only authorized parties can read it. Encryption does not itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the data is encrypted using a computer encryption algorithm, generating cypertext that can only be read if decrypted. The algorithm generally uses a pseudo-random encryption key.

In principle it may possible to "break" or decrypt a message without possessing the key, but, for a well-designed algorithm, enormous computational resources are required. However, the actual ability to decrypt depends on several factors, including the quality of the algorithm, the key length and others. Even where decryption without the key is potentially possible, the demands on computational resources may be so great that the task of decrypting large amounts of encrypted material is impossible. As vastly greater amounts of encrypted material are generated, this becomes an even more insurmountable task.[91] Looking five or ten years into the future, it is certain that the volume of encrypted material will only increase by orders of magnitude.

Key Length and Distribution: Keys are critical components of any cryptographic system.[92] The "key" is a piece of information that determines the functional output of the cryptographic algorithm. It specifies the transformation of plaintext into cipher text, and

[90] In cryptography, a cipher is an algorithm for performing encryption or decryption of data. Encryption is the process of converting data with the cipher or code. Technically, codes generally substitute different length strings of characters in the output, while cyphers generally substitute the same number of characters inputted. There are exceptions and some cypher systems may use slightly more or less characters. In the old days, commercial codes used a large codebook that substituted a random string of characters or numbers to a word or phrase. For example, "JQMZB" could be the code for "ship the goods tomorrow." In reality users of these codes were more interested in saving money on telegrams than privacy or security.

[91] An intelligence service, such as the NSA, would need to identify specific encrypted items before dedicating the computational resources needed, if it was in fact even possible for the cryptosystem employed. Such as task has become increasingly difficult in a world where almost everything is encrypted.

[92] See, Elaine Barker and Allen Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST.SP.800-131A Rev1, (November 6, 2015).

vice versa. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

End-to-End Encryption: Much of the present discussion revolves around what is called "end-to-end encryption" (E2EE) whereby only the communicating parties can read the messages or access the data involved.[93] This would, in principle, prevent anyone else, including service providers, from being able to obtain the cryptographic keys needed to access communications or data. Such systems are designed to defeat any attempts at unauthorized access or surveillance of data stored or in transit since no third parties can decipher the data being communicated or stored.

At present most server-based Internet communications do not include E2EE, and at best they only protect communications between clients and servers. Therefore, users need to rely on their commercial service providers with the original data. E2EE is generally regarded as safer because it largely eliminates the potential for other parties to access the data. Increasingly user applications, such as instant messaging, are being offered with this functional capability. Users may use a third party client (*e.g.*, Telegram or WhatsApp) to implement an E2EE scheme over a protocol that otherwise does not provide this capability inherently. In the future it is highly likely that user demand for E2EE will make such systems pervasive.

Processing Power: A major factor in the use of effective encryption and its proliferation in the digital world lies in the fact that all devices, from smartphones to large computers, contain increasingly powerful general purpose processors. This is a technology path that will continue to develop.[94] For decades encryption has not required costly electromechanical devices, and for over a decade not even specialized computer chips are required. The most powerful encryption algorithms and applications can be easily implemented on any device.

Encryption Algorithms and Applications: The heart of any encryption scheme is the computer algorithm by which the plaintext digits are scrambled into the encrypted form. Within the U.S. such algorithms have been developed at the NSA for securing government

[93] See Andy Greenberg, "Hacker Lexicon: What is End-to-End Encryption?" *Wired*, November 25, 2014.

[94] It may be the case that Moore's Law, which describes the periodic doubling of processing power, may finally be coming to an end. However, new devices will continue to become more powerful and complex. A key issue in the future for portable devices may be what processing actually takes place within the device, and what will take place at the connected service provider.

secrets, and by cryptographic researchers at universities and commercial firms.[95] Discussion of the various types and grades of these algorithms is technically complex, but it is safe to say that the overall "quality" of the algorithms now being employed for commercial purposes is relatively high-grade and will continue to improve. In the future advances in techniques such as quantum cryptography will further improve the quality of available encryption technology.

It is also the case that relatively high-grade cryptographic software is available from non-U.S. firms, including some from former Soviet cryptologists. Where some in the U.S. still operate under the delusion that it is somehow possible to "control" the proliferation of encryption software, either by statute within the U.S. or by international agreement such as the Wassenaar Arrangement, most authorities agree that this is simply not possible.[96]

Security systems are designed with the assumption that the details of the cryptographic algorithm are already available to a potential attacker.[97] A key is often easier to protect since it is generally a small piece of information (as opposed to an encryption algorithm), and easier to change if compromised. Thus, the security of an encryption system relies on at least some part of the total key being kept secret. This is one of the most difficult practical problems of managing any cryptographic system. An attacker who obtains the key by any number of means, such as theft, extortion, dumpster diving, assault, torture, or social engineering, can recover the original message from the encrypted data.

For years the U.S. Government attempted to exercise control over key lengths as one means of assuring continued access. In years past a key length of 80 bits was generally considered the minimum for strong security with symmetric encryption algorithms. Later 128-bit keys became common and were considered very strong. Even more recently longer keys have come into use. Going forward there are no longer any legal or technical constraints on keys or key length.

In public key cryptography, the keys have a mathematical structure. Public keys used in the RSA system, for example, are the product of two prime numbers and therefore

[95] While most of what the NSA does is classified, they have made public that at least four levels or types of encryption algorithms are used for various requirements.

[96] See Granick, o*p. cit.* See also, Sergey Bratus, *The Wassenaar Arrangement's intent fallacy* (December 8, 2015).

[97] This is known as Kerckhoffs' principle — "*only secrecy of the key provides security*," or, reformulated as Shannon's maxim, "*the enemy knows the system.*" The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret (see security through obscurity).

public key systems require longer key lengths than symmetric systems for an equivalent level of security.[98] Elliptic curve cryptography may allow smaller-size keys for equivalent security, but these algorithms have only been known for a relatively short time, and current estimates of the difficulty in searching for keys is still subject to dispute among technical experts.

Attacking the End Points: Much of the present discussion involves E2EE: the data is encrypted at the point of origin and subsequently decrypted at its destination by an authorized recipient. The focus has been on the possibility of "breaking" the encrypted text or somehow forcing a commercial provider to provide unencrypted access. Some experts, however, look to the fact that at some points in the process the data is either not yet encrypted, or needs to be decrypted for reading or processing. Experts look to these endpoints as a means that can be utilized to access data. In reality, this endpoint might be the connection between the keyboard and the computer, or another interface or piece of software. The question then becomes one of designing exploits or tools that access the endpoints before the initial process of encryption takes place or that hijack the user's processing software to decrypt stored information.

[98] Here 3,072 bits is considered a good key length for systems based on factoring and integer discrete algorithms which aim to have security equivalent to a 128 bit symmetric cipher.

7. Access—Backdoors, Exploits and Other Forms of Intrusion

Access to encrypted material without the appropriate key remains a fundamental problem for the Intelligence Community and law enforcement agencies that have a legitimate need for access.[99] For decades the NSA and others have employed cryptanalysts or "codebreakers" to try and accomplish this complex and difficult task.[100] As the quality of cryptographic systems and the volume of encrypted material used has increased, this community has looked to a number of potential technical solutions. The precise nature of these activities remains classified for the obvious reasons, but it is nonetheless possible to consider the possibilities in general terms.

Backdoors: A "backdoor" is a method, often secret, of bypassing the normal authentication processes required by a computer system, cryptosystem or algorithm. Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems. Operationally, these may take the form of a hidden part of an existing program, a separate program to subvert the system through a rootkit, or a hardware feature.

Normally backdoors are surreptitiously installed, but on others they are deliberate and widely known. These kinds of backdoors might have "legitimate" uses such as providing the manufacturer with a way to restore user passwords.[101] There are also cases where the U.S. Government has given approval to a new encryption standard that contains a glaring weakness which makes an encryption algorithm susceptible to cracking. Indeed, in one recent case, the government approved an algorithm with properties such that if one were intent on inserting a backdoor the algorithm was susceptible to cracking by design.[102]

[99] The extent to which such access is currently seen as legitimate under U.S. and foreign law is considered elsewhere in this study.

[100] See Kahn, *op. cit.*

[101] When the U.S. Government in 1993 unsuccessfully attempted to deploy an encryption system, the Clipper Chip, this technology contained an explicit backdoor for intelligence and law enforcement access.

[102] See, for example, Kim Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA" *Wired*, September 24, 2013. Also the *New York Times* reported a leak by Edward Snowden, which

Exploits: Closely related to the concept of backdoors are "exploits" which are pieces of software, a chunk of data, or possibly a sequence of commands that take advantage of a set of vulnerabilities in order to cause unintended or unanticipated behavior to occur on computer software or hardware. Most commonly such behavior includes gaining control of a computer system through allowing unintended access, information leakage, or privilege escalation. Exploits are generally designed to provide superuser-level access to a computer system, although it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root. For currently maintained software there is often a team responsible for eliminating vulnerabilities through software patches distributed to customers or the general public, along with building larger scale mitigations against whole classes of vulnerability types and generally improving software quality over time.

Presently a subject of policy discussion are so-called "zero-day exploits," which exploit an existing vulnerability that are previously unknown to the public or the software vendor. Most zero-day exploits can use a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves no opportunity for detection at first. A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day." The attacker writes and implements exploit code while the vulnerability is still open and available.

After releasing the exploit, it can be recognized in the form of identity or information theft or possibly by a developer who catches it and creates a patch to stop the attack. Once a patch is written and used, the exploit is no longer called a zero-day exploit. Such attacks are rarely discovered right away, and are therefore a cause for concern. In actuality it may take not just days, but months and sometimes years before a developer learns of the vulnerability that led to an attack.[103]

---

apparently confirmed that a weakness in the standard and so-called Dual_EC_DRBG algorithm was indeed a backdoor. The *Times* story implies that the backdoor was intentionally put there by the NSA as part of a $250-million, decade-long covert operation by that agency to weaken and undermine the integrity of a number of encryption systems used by millions of people around the world.

[103] As mentioned previously, one estimate is that it currently takes an average of 312 days for cybersecurity experts to manually detect a new zero-day exploit, and then develop a "patch" for it. This disturbing fact was one compelling reason for DARPA to undertake a program whereby supercomputers could be programmed to detect and patch such vulnerabilities in seconds. This technology was recently demonstrated

There are many implications to the discovery and use of zero-day exploits which impact public policy. Currently many parts of the country's critical infrastructure are so unprotected that even one vulnerability (zero-day or not) can be used to cause great damage. Programs that strategically harden both the national infrastructure and government agencies against vulnerabilities require massive study and immediate implementation to avoid systemic risks from malicious nation states or other third parties.

Vulnerability Equities Process (VEP): The government has established a Vulnerability Equities Process (VEP) to determine whether to withhold or disclose information about computer software security vulnerabilities. Under the VEP, the government will evaluate whether to disclose a vulnerability it has obtained or discovered—so that the software developer has a chance to fix the problem—or the government may choose to withhold the information to use it for purposes including law enforcement, intelligence gathering, and "offensive" exploitation.[104]

Current policy towards vulnerabilities attempts to balance U.S. interests by way of the NSC-run Vulnerability Equities Process (VEP), which under current stated policy runs every discovered vulnerability through a series of workflows designed to lean towards disclosure but save those vulnerabilities needed for the Intelligence Community's SIGINT collection efforts. Solving the "going dark problem" and future-proofing the nation's SIGINT collection ability is going to lean on this capability more than can be stated here

at the 2016 "DARPA Cyber Grand Challenge." While the proof-of-concept was successfully demonstrated, operational programs against current exploits may be years away. Some experts question whether such a system could ever be developed to the point where it could be operationally deployed.

[104] The VEP began in 2008 when a group was created to develop a Joint Plan for improving the government's ability to use offensive capabilities against U.S. adversaries and to protect both government and public information systems, although it did not become public until 2016. This group subsequently recommended adoption of the VEP. Between 2008 and 2009, the DNI led another working group to addressing the VEP recommendation, producing a report entitled *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, later referred to as the VEP and created a group with within the NSA to oversee the VEP. In 2013, the President's Review Group on Intelligence and Communications Technologies concluded that the government should not continue to exploit zero-days but instead should disclose all vulnerabilities, except where there is a clear national security need to retain the exploit, based on a belief that disclosures were not happening to the degree that they should and that the oversight procedure was flawed and recommended that the NSC take over the zero-day decision-making process.

and the U.S. Government will likely need to realign policy to ensure the process continues to support critical national security requirements.

While exploits are often seen as the domain of "black hat hackers," nefarious individuals who seek to do harm or engage in criminal acts, they are also designed by "white hat hackers" who are part of the cybersecurity industry or the Intelligence Community seeking access to protected data. The extent to which these efforts may be successful over the long term against the ongoing technology path in the encryption area remains a fundamental question in the "going dark" debate.

Quantum Computing: One potential approach to solving encryption problems lies in the field of quantum computing (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.[105] At present the development of actual quantum computers is still in its infancy, although experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits, and the government continues to fund quantum computing research for a variety of difficult problems, including cryptanalysis.

Large-scale quantum computers would theoretically be able to solve some difficult problems far more quickly than classical computers that use even the best currently known algorithms, like integer factorization.[106] There exist quantum algorithms, such as Simon's algorithm, that run faster than any possible probabilistic classical algorithm. Given

[105] Quantum computers differ from digital electronic computers in that digital computing requires that the data are encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1) and quantum computation uses quantum bits, which can be in superpositions of states. Quantum computing began with the work of Paul Benioff and Yuri Manin in 1980, Richard Feynman in 1982, and David Deutsch in 1985.

[106] Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers. By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This might allow a quantum computer to decrypt many of the cryptographic systems in use today. In particular, some public key systems are based on the difficulty of factoring integers or the discrete logarithm problem, both of which can be solved by Shor's algorithm. In particular the RSA, Diffie-Hellman, and Elliptic curve Diffie-Hellman algorithms could be broken. These are used to protect secure Web pages, encrypted email, and many other types of data. However, other cryptographic algorithms do not appear to be broken by those algorithms. Some public-key algorithms are based on problems other than the integer factorization and discrete logarithm problems to which Shor's algorithm applies. Lattice-based cryptosystems are also known to not be broken by quantum computers.

sufficient computational resources, a classical computer could, in theory, simulate any quantum algorithm, as quantum computation does not violate the Church-Turing thesis. On the other hand, quantum computers may be able to efficiently solve problems which are not *practically* feasible on classical computers. On balance, however, most experts agree that even if quantum computing becomes a reality, it would only be useful against a limited subset of encryption problems.

Social Engineering and Insiders: Often the user is the most vulnerable link in data security. Successfully impersonating legitimate users to reset passwords or otherwise gain authenticated access to an account generally also provides access to encryption keys and thus information in plaintext. Insiders with access may remove data over networks or connected storage devices. Alternatives to passwords, including biometrics, have their own problems and vulnerabilities. Usage monitoring can reduce the extent of damage from ordinary insider users, but is not likely to as readily reduce vulnerabilities to superusers with direct machine level access.

8. "Going Dark" and Unintended Consequences

Security, Privacy and the Technology Path: One fundamental point of this analysis has been the fact that the world is on a technology path with no turning back to antiquated media, and users who have lost control of their data are making increasing demands for privacy and security. While few anticipated the speed or magnitude of the technology revolution, neither the government nor the private sector moved to meet these user demands and provide adequate technical solutions in a timely manner.

Over time at least some of the current cybersecurity problems will be "solved" because a large class of users demand it and technical solutions can be implemented to deal with the most glaring known and evolving vulnerabilities. At the same time virtually all software and human systems contain defects that can be exploited, and there will be continued development of new exploits to take advantage of these opportunities. The dynamic competition between cybersecurity and exploit development will continue. Questions remain as to what resources are devoted to either side of the competition.

Clearly much remains to be done in the policy domain, funding and implementation of effective solutions.[107] As effective cybersecurity is recognized as a "public good" there is good chance that additional guidance and funding will be provided to agencies such as DARPA, NSA, CYBERCOM, and other government agencies to develop the needed technologies in partnership with the commercial sector.[108] Thus far the government has failed to both assign this critical mission to these agencies and provide the resources needed to accomplish the tasks involved.

[107] Fortunately these are not partisan issues. Hopefully the new Trump administration will take the next necessary steps to formulate and implement a comprehensive cyber policy.

[108] One example here is the BRANDEIS Program recently initiated at DARPA. However, guidance provided in PPD-21 on this subject fails to even mention DARPA or the Defense Department at all. While this Directive assigns the cybersecurity mission responsibility to the Department of Homeland Security (DHS) and the National Institute for Standards and Technology (NIST), there appears to be little in the way of program coordination among these agencies and the various DoD components. Neither DHS nor NIST have the management or technical infrastructure required to execute the scale of a program required. They also lack the legal authority needed under Title 10 and Title 50 of the U.S. Code.

User demands, including individual and institutional outrage over some of the more recent attacks on various systems, can be a major driver of the availability of more secure systems and protocols. This is particularly the case because service providers are often unable to provide levels of privacy and security now demanded. Near-term solutions, such as specialized security applications, only serve as a temporary fix in an arena where more global solutions are required. However, it can be expected that while better solutions will be on the market and will be taken up by those most concerned for privacy, including sophisticated terrorists and criminals, the vast majority of commercial and public users (and, hopefully, criminals and terrorists) will for some time not avail themselves of the best available technology.

For the near term, however, the solution will not be binary, *i.e.*, cyberspace will not be totally secure and new vulnerabilities, such as zero-day exploits and sophisticated denial of service (DDoS) attacks, will arise that cannot be avoided completely. In the five to ten year time frame the majority of known and anticipated vulnerabilities can likely be dealt with. However, the specter of a "cyber Pearl Harbor" continues to loom.[109] It is increasingly evident that potential adversaries in the cyber domain such as Russia, China, Iran and North Korea, for example, continue to develop their cyber espionage and cyber warfare capabilities.

The Longer Term: In the best of all possible worlds, the most glaring cybersecurity and privacy problems could not be solved in the near-term even with large scale resources for DHS, NIST, DARPA, NSA and the technology sector. Qualified technical staff and management teams simply do not exist in the numbers needed. At the same time, these are tractable problems which can be solved over a longer term with significant investment in three major areas: first, a new Internet architecture which moves away from antiquated and vulnerable protocols; [110] and second, encryption that is a central feature of operating systems, data storage, transmission and all other aspects of the coming era in cyberspace.

[109] The concept of a "digital Pearl Harbor" or "cyber Pearl Harbor" has been the subject of much discussion at least since 2002 when the U.S. Naval War College conducted an exercise with that name. The general concept is one where a hostile actor launches a coordinated cyberattack on U.S. infrastructure, including SCADA systems, such as the power grid; the financial sector; communications as well as other elements connected to the Internet. While the result of the 2002 exercise saw this as unlikely, the potential and probability of such an attack has increased significantly since then.

[110] Most experts agree that the current Internet Protocol version 6 (IPv6) fails to address many of the more serious problems.

The third critical area is the need to invest in the educational system to support the need for skilled programmers and management personnel for cybersecurity efforts. Included here are undergraduate, graduate as well as post-graduate programs in much the same way the nation met the challenge of the "space race" in the 1960s.

Legal and technical limitations that existed in earlier times have now vanished and user demands have increased greatly. The question now is not whether these limitations and demands exist, but rather how soon they will increase and what will be the nature of this new world. For purposes of analysis, this study has examined not only the current world, but also the likely state of the world eighteen months away, five years away, and finally ten years away.

"Going dark" is going to become technical reality, most likely not in the next eighteen months, but almost certainly by the end of the coming decade and needs to be an essential part of the planning government process.[111] End-to-end encryption of all communications and data, differential privacy, and secure communications for all users, are likely to be the new reality. This is the technology path that cannot be stopped and one which certainly has a number of unintended consequences. At the same time, however, plaintext information in any capacity (from notes to contact lists to documents) will only ever exist on unlocked/decrypted, client held, end point devices and are rarely at rest or in transit. The opportunity to acquire that information will only exist in a window of time when that device is unlocked.

To what extent lawful access by the Intelligence Community, law enforcement agencies, or hackers, employing new and sophisticated exploits will be possible remains an ongoing discussion, much of which is not open to public view. A general consensus, however, suggests that even where some access may be possible, it will be a highly limited and costly enterprise. By and large the "Golden Age of SIGINT" is over.

Unintended Consequences: The heart of the debate really is about what "going dark" means in serious technical terms and the consequences, intended or not, of this new reality. Clearly what the security and "information assurance" community is working toward is a digital world where user data is secure and protected from a range of threats. No one doubts that this involves encryption at various points in the process as well as new

[111] Here the eighteen-month time horizon has been used as it is the generally accepted length of a single generation in computers and related technologies.

software systems. What may be unintended here is the extent to which this level of privacy and security impedes the needs of law enforcement and intelligence agencies.

As mentioned, FBI Director James Comey, Congressman Adam Schiff, and others openly speculate that for law enforcement and intelligence there is no obvious technical solution. Indeed, Schiff sees this as the largest challenge currently facing the Intelligence Community. Opposing this pessimistic view are others, such as former DNI James Clapper, who dismiss the problem as being "overhyped" and (incorrectly) point to the fact that the SIGINT community has always found ways to access needed materials. Where there is no disagreement, is that the "going dark" debate will likely go on for some time.

The many methods for controlling use of encryption technology previously available are no longer available or are now irrelevant. It is important to structure a technical environment and legal regime that allows legitimate access to encrypted materials, particularly over the long-term. However, the concept of forcing commercial firms and service provider to provide access to user data by court order or otherwise is simply not viable in a world where it is no longer possible for them to do so.

Dealing with the unintended consequences of this new digital order then becomes one of non-cooperative technical access. Here there are two major hurdles. The first involves the development of technical tools such as exploits that can "break" or otherwise work around the nature and volume of encrypted materials. The second will be overcoming ever increasing concerns about privacy and the efforts by both the Congress and the courts to constrain surveillance activities by various government agencies. While at present this may be easier for NSA than the FBI, it is unclear that either agency will be in a good position to operate in this area ten years from now.[112] At best, technical access where possible may be a very limited and costly enterprise.

FBI Hacking with NIT to Overcome Encryption: As demonstrated through the so-called "Playpen" cases, the FBI has used a tool called a network investigative technique (NIT), which essentially means hacking, to overcome problems posed by encryption. In February 2015, the FBI seized the server running a bulletin board site on the dark web,

[112] The various cases the FBI has which require "breaking into" iPhones for criminal cases are instructive examples here. Filings by both the government and Apple in the *FBI v. Apple* case related to the San Bernardino terrorist incident, as well as the amicus filing by the EFF, provide considerable insight. Unable to access the terrorist's phone, the FBI was able to "outsource" the problem to a commercial security firm, reportedly in Israel, that was able to access this phone. However, the firm stated that it would be unable to do so for newer releases of the iPhone's operating system.

Playpen, which featured child pornography and then continued operating Playpen from its own servers.[113] From February 20, 2015 to March 4, 2015, the FBI deployed a NIT to visitors who logged into the website and was able to identify 1,300 true IP addresses. This investigation has led to more than one hundred criminal cases filed around the United States, but the various federal judges assigned to the cases have differed in their approaches.[114]

Most notably, some judges have found that, instead of the single search warrant obtained for deploying the NIT, the FBI needed search warrants for each account that was hacked in order to comply with the Fourth Amendment. In addition, some have found that the warrant violates Rule 41 of the Federal Rules of Criminal Procedure since warrants must be issued only in the judicial district where the judge is located.[115] In the Playpen cases, the magistrate judge who issued the warrant was located in the Eastern District of Virginia, which is where the FBI was temporarily running the server but obviously not where all of the site visitor's computers were located.

A second area of concern stems from the evolving nature of the law in the privacy area and continued expansion of Fourth and Fifth Amendment protections to searches and surveillance. While this may be more of a concern to domestic law enforcement than intelligence operations, recent battles over Sections 215 of the USA Patriot Act and 702 of the FISA Amendments Act of 2008 demonstrate that the Intelligence Community is not immune either. Cases in this area are still in the courts, and major decisions by the Supreme Court can be expected in the next year or two. This too is an unsettled area, but one where at least the trend is strongly in favor of privacy advocates.

Alternative Sources and Methods: The general response to the prospect of losing access to communications and data by technical means, commonly referred to as SIGINT,

[113] Joseph Cox, "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers," *Vice – Motherboard* (January 5, 2016). http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

[114] Electronic Frontier Foundation, *The Playpen Cases: Frequently Asked Questions* (last visited October 26, 2016). https://www.eff.org/pages/playpen-cases-frequently-asked-questions.

[115] However, the proposed change to Rule 41, effective December 1, 2016 pending Congressional approval, expands the reach of magistrate judges to include "the district where the media or information is located has been concealed through technological means" or when the media are on protected computers that have been "damaged without authorization and are located in five or more districts." Supreme Court of the United States, Letter on Amendments to the Federal Rules of Criminal Procedure (April 28, 2016), https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.

is to invest more heavily in other sources of information, such as human sources. These are traditionally known as HUMINT. While well-intentioned, this is far easier said than done, particularly in light of the problems facing the Intelligence Community these days.[116] In the current era a host of additional problems arise here, including electronic identity management and records comparisons across neighboring and cooperating countries; difficulty in maintain asset covers in the digital world; as well as the difficulty in bypassing electronic border controls and biometrics.

Another alternative, and not mutually exclusive with enhanced HUMINT, is more extensive collection and exploitation of data which is not encrypted and flooding the Internet in ever greater amounts, largely through social media. Collection of this "open source" data or OSINT has traditionally been the poor stepchild of the intelligence business may ultimately prove to be its salvation. While Internet users are demanding greater privacy and security of their personal data, they also engage in the posting of vast amounts of information on a wide range of social media sites, such as Facebook and a host of others, which can be easily collected. Notwithstanding various legal challenges to the collection and mining of this readily available data, the coming decade will certainly see more effective mining and analysis of this information for legitimate law enforcement and intelligence purposes.

[116] It is also the case that such suggestions are made by people who lack a good understanding of this area. This is an area where the U.S., as well as its allies, can and should make ongoing investments. However, by its very nature results are often unpredictable and by no means guaranteed. At best, it is a highly risky and uncertain enterprise.

Study Team

Lillian Ablon	*The RAND Corporation*
David Aitel	*Immunity, Inc.*
Sofia d'Antoine	*Trail of Bits*
Edward Doyle	*Center for Advanced Studies on Terrorism*
Thomas Garwin	*Center for Advanced Studies on Terrorism*
Daniel Guido	*Trail of Bits*
Nicholas Rostow	*Yale Law School*
Ryan Stortz	*Trail of Bits*
Mara Tam	*QxNch*
Abraham Wagner	*Columbia Law School*
Kevin Yorke	*New York County District Attorney's Office*

Research Assistants

Jacob Arber	*Columbia Law School*
Christine Chen	*Columbia Law School*
Theodore Rostow	*Yale Law School*
Kathryn Witchger	*Columbia Law School*

References

Banisar, David, *Stopping Science: The Case of Cryptography*, 9 *Health Matrix* 253 (1999).

Barker, Elaine and Allen Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST.SP.800-131A Rev1, (November 6, 2015).

Bellovin, Steven, "Frank Miller: Inventor of the One-Time Pad". *Cryptologia* 35 (3): 203–222 (2011).

Brody, Sara Sinclair, *Protecting Data Privacy With User-Friendly Software,* Council on Foreign Relations Cyber Brief (May 2016).

Carlin, John P., "Detect, Disrupt and Deter: A Whole-of-Government Approach to National Security Cyber Treats," 7 *Harvard National Security Journal* 391 (2016).

Chatzikokolakis, Konstantinos, et al, "Broadening the scope of Differential Privacy using metrics." *Privacy Enhancing Technologies*, (Berlin-Heidelberg: Springer, 2013).

Childe, Kerry L., *Cybersecurity and Privacy: Three Federal Proposals*

Cryptography's Role in Securing the Information Society, (Nat'l Academies Press 2016).

Danzig, Richard J., *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Center for New American Security, 2015).

Department of Defense, *DoD Cyber Strategy* (April 2015)

Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013).

Deibert, Ronald J., *Black Code: Surveillance, Privacy and the Dark Side of the Internet,* (McClelland & Stewart, 2013).

Don't Panic: Making Progress on the "Going Dark" Debate, (The Berkman Center for Internet and Society at Harvard University, February 2016).

"Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependent on Aps, Software – Kik, Surespot, Telegram, Wickr, Detekt, Tor," *Inquiry & Analysis Series Report No. 1168,* Middle East Media Research Institute (MEMRI)(June 16, 2015).

Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, 80 Fed. Reg. 18,077 (April 1, 2015).

Executive Order ____, *Strengthening U.S. Cybersecurity and Capabilities* (January 27, 2017).

Ghosh, A., T. Roughgarden, and M. Sundararajan. "Universally utility-maximizing privacy mechanisms." *Proceedings of the 41st annual ACM Symposium on Theory of Computing*, (New York: ACM, 2009)

Goldreich, Oded, *Foundations of Cryptography*: (Cambridge University Press, 2004)

Goldsmith, Jack and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006).

Gorski, Ashley and Patrick C. Toomey, *Unprecedented and Unlawful: The NSA's "Upstream" Surveillance* (American Civil Liberties Union, September 19, 2016).

Greenberg, Andy, "Hacker Lexicon: What is End-to-End Encryption?" *Wired*, November 25, 2014.

Harrison, Richard M. and Trey Herr (eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age* (New York: Rowman & Littlefield, 2016).

Into the Grey Zone: The Private Sector and Active Defense against Cyber Threats (The George Washington University, Center for Cyber and Homeland Security, October 2016).

Kahn, David, *The Codebreakers - The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1967)

Kerr, Orin, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 505 (2001).

Landau, Susan, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, The MIT Press, 2013).

Leary, Mary G., *Katz on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 Am. Crim. L. Rev. 356-361 (2013).

Levy, Steven, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (New York: Viking Penguin, 2001).

Marczak, Bill and John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

McLaughlin, Jenna "Spy Chief Complains The Edward Snowden Sped Up Spread of Encryption by 7 Years," *The Intercept* (April 25, 2016).

Miller, Frank Miller, *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. (C.M. Cornwell, 1882)

Olson, Mancur, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, Harvard University Press, 1971).

Perera, Tom. *The Story of the ENIGMA: History, Technology and Deciphering, (2nd Edition),* (Artifax Books, 2004)

Presidential Decision Directive/NSC-63, *National Infrastructure Protection*. (May 1998).

Presidential Policy Directive/PPD-21. *Critical Infrastructure Security and Resilience.* (February 12, 2013).

Presidential Policy Directive/PPD-41. *U.S. Cyber Incident Coordination.* (July 27, 2016).

"Proposed State Bans on Phone Encryption Makes Zero Sense," *Wired* (January 16, 2016).

Report to the President: Big Data and Privacy: A Technological Perspective (May 2014).

Rogin, Josh, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy* (July 9, 2012).

Schneier, Bruce, *Applied Cryptography*. New York: Wiley, 1995.

Schneier, Bruce, *Someone is Learning How to Take Down the Internet*, Lawfare.com.

Vagle, Jeffrey L., *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 *Ind. L.J*. 101, 109 (2015).

Wagner, Abraham, "Cybersecurity: From Experiment to Infrastructure, *Defense Dossier* (August 2012).

Wagner, Abraham R., *Cybersecurity, Cryptology, and Privacy in Historical Context: The Challenge of New Technologies and Media,* Paper Presented to National Security Agency Cryptologic Symposium (October 2013)

Wagner, Abraham R. and Nicolas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2016).

Wagner, Abraham R., *Cybersecurity and Privacy: The Challenge of Big Data*, Paper Presented to the Office of Technology Assessment (Executive Office of the President), Big Data Study (March 2014)\

Wagner, Abraham R., *Cybersecurity: New Threats and Challenges* (American Foreign Policy Council, 2013)

Wagner, Abraham R. and Paul Finkelman, "Security, Privacy and Technology Development: The Impact on National Security," *Texas A&M Law Review* (2016)

Whitten, Alma and J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* (Carnegie Mellon University, 1998).

Winterbotham, F.W. *The Ultra Secret.* (London: Weidenfeld & Nicolson, 1999).

Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel "Unique in the Crowd: The privacy bounds of human mobility." *Nature* (March 25, 2013).

WORLD WIDE WEB CONSORTIUM, *Securing the Web* (Jan. 22, 2015), available at https://www.w3.org/2001/tag/doc/web-https

Zdziarski, Jonathan, "Apple, FBI, and the Burden of Forensic Methodology," (February 18, 2016)

Zetter, Kim, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA" *Wired*, (September 24, 2013).

Zetter, Kim, "How the Feds Could Get Into iPhones Without Apple's Help," *Wired* (March 2, 2016).