The Software Alliance

BSA

# ENCRYPTION:
## Securing Our Data, Securing Our Lives

### HOW IT WORKS AND WHAT IT DOES

## Introduction

The widespread availability and use of security technologies, most notably encryption, is an essential feature of our increasingly connected digital world. Every time we log into our bank accounts or favorite social media site; every time we make a cell phone call to a loved one; every time we pay for something with a credit card; and every time we upload pictures, documents, and records to the cloud, our data is being protected by encryption. And it is not just the content we create or the communications we initiate. Encryption is used to prevent hackers from accessing our health records or wreaking havoc with our transportation infrastructure and electrical grid.

***Encryption is used to prevent hackers from accessing our health records or wreaking havoc with our transportation infrastructure and electrical grid.***

Encryption has been around for centuries. Yet only now has the demand for security and privacy converged with the availability of new technologies, resulting in encryption taking its central position of enabling our dynamic, digital world today.

This paper describes the vital but often unnoticed role encryption plays in our daily lives — whether protecting our personal information and banking data, driving economic opportunity, or guarding our nation's critical infrastructure. It explains how encryption works, how it is used, what makes it strong, and why efforts are underway to continuously improve digital security and enable new opportunities.

Although its role is often overlooked, encryption empowers us to take the most important, intimate, and sensitive information in our lives, and makes sure we can control what happens with it — even if a device is lost or stolen. Encryption does not just protect our privacy, it also is used to improve security, ensure identity, and protect anonymity. With more and more wearables coming to market tied to fitness and good health, encryption is even able to protect the private moments when our hearts race and our feet walk.

# THE ROLE ENCRYPTION PLAYS IN OUR LIVES AND OUR ECONOMY

Although we may not think about encryption every day, it has become an important and often hidden driver for various critical activities we take for granted. Imagine two busy parents going about their day. It's a big day for Jane and John Doe.

## A DAY IN THE LIFE WITH ENCRYPTION

Jane wakes up first to go for a run, and has her smartphone log her steps and keep track of her heart rate at various intervals.

Before leaving for work, John helps their daughter finish her history paper, which is stored in the cloud for her teacher to review.[1]

At the same time, Jane remotely logs into work[2] and checks her e-mail.[3]

She texts her client[4] and they pick a location to meet for lunch.[5]

Jane gets to the restaurant early and uses its Wi-Fi[6] to browse the Internet.[7]

She pays for lunch with a credit card.[8]

Before leaving she checks her smartwatch[9] and sees that she still has time to stop by the ATM.[10]

Meanwhile at work, John goes online to check the results of a recent medical test showing good news.[11]

John makes a cellphone call to his wife to let her know.[12]

He logs into their bank account[13] to see if Jane's paycheck has been deposited yet[14] before deciding to purchase tickets for their long-delayed vacation.[15]

When Jane and John get home, they warm up with their connected thermostat,[16] rent a movie from their cable TV provider,[17] and post a funny animated gif to Twitter.[18]

It has been a long day, and they fall asleep to a favorite playlist from their streaming music service.[19]

Each of these moments, and many more in our busy lives, are enabled by encryption.

**Encryption plays an increasingly vital role in helping to grow our economy.** The widespread use of the various forms of encryption is enabling us to do things never before possible, and, as a result, is fueling near unprecedented growth in the digital economy.[20] Encryption is helping protect billions of online transactions each day, enabling banks to route more than $40 trillion in financial transactions a year, and enabling consumers to order more than $300 billion in online goods and services with just the click of a button.

*By guarding our most vital computers and networks from intrusion, encryption has been at the forefront of efforts to make our information infrastructure more secure, trustworthy, and resilient.*

Its effect is being felt throughout the economy in nearly every sector where securing information is necessary. For example:

- In the energy sector, encryption is at the heart of SmartGrid technologies that promise to reduce greenhouse gas emissions and boost network reliability.

- In the health care sector, leaders are turning to encryption to help better protect the privacy of patient data,[21] and to enable a cloud-driven revolution in personalized medicine that promises to help people live longer, healthier lives.[22]

- In the transportation sector, connected vehicle technologies, which rely on strong encryption to prevent the cars from being hacked, may be used to cut highway fatalities in half.[23] Today's cars can already contain as many as a 100 million lines of code — 100 times more than the space shuttle had when it launched.[24]

**Encryption has been at the forefront of protecting our most vital national security secrets for years.** Encryption technology has long played a crucial role in protecting US national security interests, from the critical role cryptographers played in our ability to win World War II, to the role encryption plays today to protect the sanctity of information that flows across classified national security networks, to the encrypted transceivers that are used to secure and control drone weapon systems.[25] By guarding our most vital computers and networks from intrusion, encryption has been at the forefront of efforts to make our information infrastructure more secure, trustworthy, and resilient.

Encryption also helps protect against the disruption of critical infrastructure systems. Businesses and policymakers alike are turning to strong encryption to safeguard our electric grid,[26] to protect the industrial control systems[27] that control our waterways,[28] to secure private nuclear facilities,[29] and to protect our air traffic control system from hackers.[30] Encryption plays an important role around the globe where it enables good people living under repressive regimes to spread freedom and hope.[31]

# Encryption 101: The Basics

Encryption is designed to help protect data whether it is sitting on a computer, residing on a phone, being transmitted across the Internet, or being stored in the cloud.

***Encryption strength is often measured by how long the key is needed to unlock it. The longer the key, the harder it is to break.***

Technically, encryption works by mathematically transforming data into undecipherable gibberish-looking text that can only be read by authorized people with the right decryption key. An encryption key is a random-looking sequence of bits that is created specifically to scramble and unscramble data.

Encryption technologies are sometimes described as being either "weak" or "strong." Encryption strength is often measured by how long the key is needed to unlock it. The longer the key, the harder it is to break.

For example, early use of 40-bit encryption keys equated to 1 billion possible keys and combinations. Attempting to crack a message with a billion possible keys sounds like trying to find the proverbial needle in a haystack. However, a typical home computer in 2004 could crack open a 40-bit key in a little less than two weeks, using what is called a brute-force attack consisting of sequentially running through an enormous number of trial and error guesses — in this case testing a million keys per second.[32] By 1998, a group of online enthusiasts found they could build a machine made of lots of CPUs to crack a 40-bit key in just two seconds.[33] Although the government at one point tried to limit encryption to this length,[34] these 40-bit keys now are considered to be dangerously weak encryption.[35]

By contrast, strong encryption uses longer keys. Take for example the 128-bit key that is frequently used to protect data at rest on a hard drive. A 128-bit key can have more than 340,000,000,000,000,000,000,000,000,000,000,000 key combinations. It is the strength of this encryption that has made it essential for protecting our digital economy and our nation's most important national security secrets, and for the resilient functioning of our nation's critical infrastructure.

Although the mathematics of encryption are robust, poor implementation can make encryption weak. Numerous factors can weaken the ability of encryption to protect sensitive data, including whether it has a short key-length, implementation flaws, bad passwords, or a weak algorithm.

# Three Fundamental Encryption Types and Their Uses

## 1. Symmetric Encryption: Protecting Data at Rest on a Device or in the Cloud

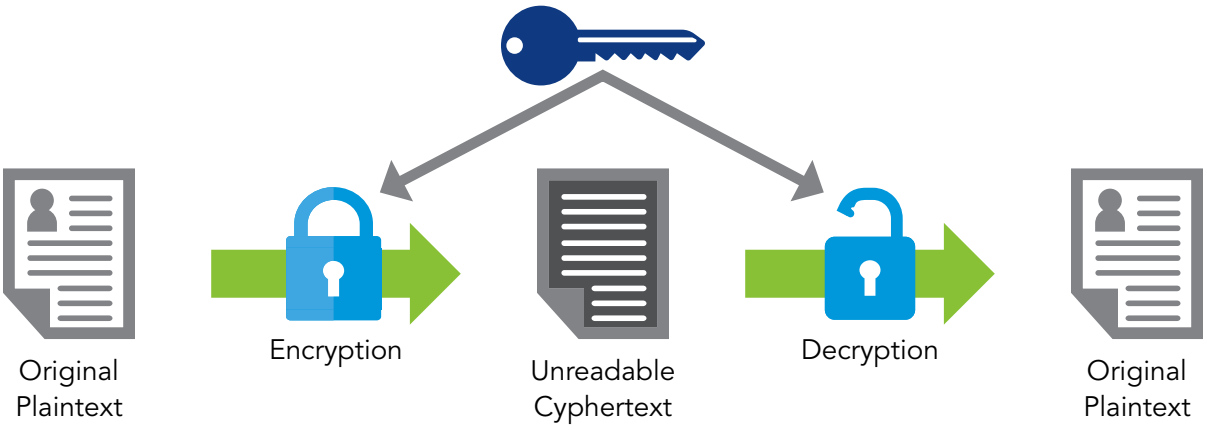
One of the simplest but strongest forms of encryption uses a "symmetric" key and is essential for protecting data, whether it is at rest on a computer or at rest on a server somewhere in the cloud. Generally, it uses the same key (or password) to encrypt and decrypt data, and is sometimes referred to as secret-key encryption. This type of technology is used to encrypt everything from an entire hard drive to an individual file. Once a file is encrypted, it can be sent or stored in the cloud — but a cloud provider would not have access to the data without having access to the original key. The primary advantage of this form of encryption is that it is fast and can be used to encrypt large volumes of static data. Symmetric keys are generally 128 or 256 bits in length.

Some examples of symmetric key encryption systems include DES, TripleDES, Advanced Encryption Standard (AES), AES-256, Twofish, Blowfish, and RC5. AES is the most popular form and is approved for protecting classified US government information.

The biggest limitation of symmetrical encryption algorithms like AES lies in their inability to adeptly share information across a network or with multiple parties. If multiple people need access to the same data, there must be a way to distribute the keys without the keys being intercepted. This makes it especially difficult to use across a network, because there generally are not secure ways to send the key across the network (without another layer of encryption). An additional downside of symmetric encryption is that often only the user has the key (not the maker of the algorithm or the device), so if a key is lost or a password is forgotten any encrypted data is likely to be unrecoverable.

**SYMMETRIC ENCRYPTION**

Same key is used both to encrypt and decrypt



## 2. Asymmetric Encryption: Protecting Data in Motion During Transmission

To overcome the symmetric encryption's limitation of sending data across the network for use by multiple parties, another type of encryption is used to protect data against prying eyes while it is in motion. Asymmetric encryption, also sometimes known as public-key encryption, uses a pair of mathematically related keys — a public key, and a private key that is never shared. These two keys are created by mathematical formulas that are easy to solve in one direction, but hard to solve in the other direction. Thus, anyone can encrypt a message using the public key (generally made available by the system provider), but only the holder of the paired private key can decipher it. This enables encrypted information to be sent and received by different people without ever having to transmit a private key, thus making the data more secure. Most asymmetric encryption systems also have the important ability to cryptographically "sign" data to prove it was signed with the private key.

Asymmetric keys are typically 1024 or 2048 bits long, although, in the asymmetric context, keys smaller than 2048 bits are no longer considered safe to use. Examples of asymmetric key encryption technologies include RSA, Elgamal, Diffie-Hellman, DSA, and Elliptic curve (ECC).

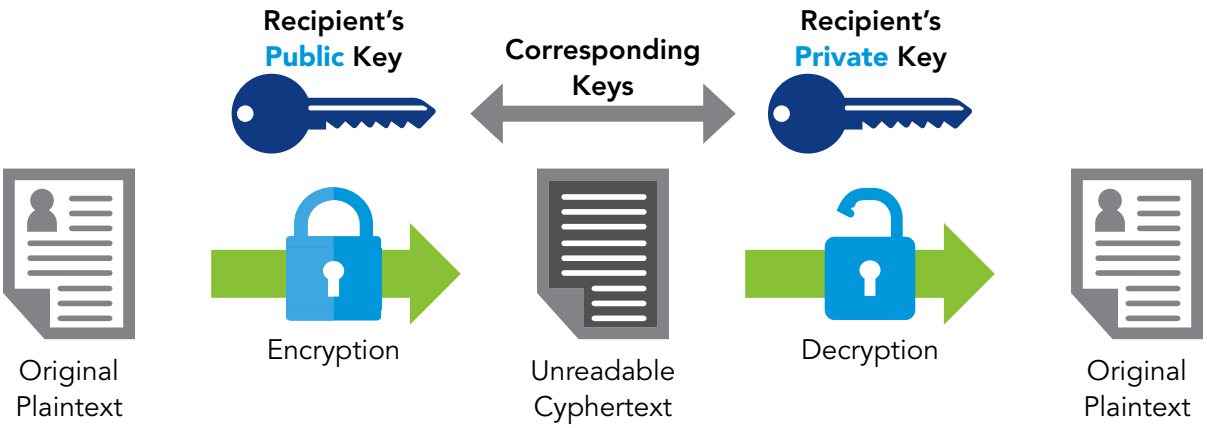
Asymmetric encryption is used in many ways. It is used to establish a secure connection between a web-browser and server. It is used to sign software updates so that your operating system, device, or software app knows that the update originated from a trusted party. And it can be used to encrypt e-mail.

Many encryption implementations may actually use a combination of symmetric and asymmetric encryption technologies to establish and protect communications. For example, technologies like Pretty Good Privacy (PGP), and OTR Ratchet (used in some common end-to-end encryption applications) are hybrid technologies.

One of the more common examples of a system that benefits from using both types of encryption is the Secure Sockets Layer (SSL) encryption that is used when your Internet browser sets up an encrypted connection with a server, and displays a small padlock in the

**ASYMMETRIC OR PUBLIC KEY ENCRYPTION**

Separate paired keys are used to encrypt and decrypt




**Anyone with a copy of your public key can encrypt information that only you can read.**

status bar. SSL now is a mainstay of the online economy, and often also is used to protect the connection between mail server and client, as well as online shopping transactions. It uses the asymmetric public key to set up the session, then passes a symmetric key that is only used for that specific session, then thrown away.

*Key escrow is a form of encryption key administration where an additional key to decrypt the data is created and held by an authorized third party in escrow.*

One important limitation that had to be overcome in the use of asymmetric encryption technologies is vulnerability from what is called a man-in-the-middle-attack. Under this scenario, a bad actor may provide you with their public key, and give the other intended recipient another public key, pretending it is yours. This enables the bad actor to insert itself in the middle of the conversation — decrypting the information in the middle before passing it along.

To overcome these challenges and ensure the correct public key is always used, the keys often are distributed by relying on either trusted software or an entity we already trust that cryptographically signs the keys. For example, secure websites must obtain a certificate for their HTTPS server from a trusted certificate authority. Because web browsers trust certificate authorities to sign keys, websites are able to send signed public keys that allow the web browser to know they can trust the public key and initiate a secure connection.

### *Key Escrow*

Key escrow is a form of encryption key administration where an additional key to decrypt the data is created and held by an authorized third party in escrow — for example, on a corporate e-mail system the company may hold it. If a key is lost or compromised, this backup key can be used to provide access to the encrypted data. This type of encryption is sometimes used by businesses[36] to protect data on a laptop in case it is stolen, and to preserve data if an employee's password is forgotten or lost.

Use of key escrow technologies has also been proposed as a solution to government access to encrypted data. In 1993, the US government proposed the novel (and highly controversial) Clipper Chip to enable law enforcement access to encrypted data. To allow easy government access, the government proposed making a copy of the key — divided in two and held by two different government agencies. One of the challenges with split-key and key escrow techniques is the sheer technical complexity of trying to create such a complex system while also keeping the keys fundamentally secure. By 1996, the Clipper Chip concept was widely rejected because of this complexity, because researchers had disclosed gaping vulnerabilities, and because it could have severely impeded online security. An AT&T researcher named Matt Blaze discovered a serious design vulnerability enabling malicious parties to disable the key escrow system at the heart of the government access system, essentially making the chips useless.[37]

Fast forward to July 2015, when more than a dozen of the world's top cryptographers published a paper warning that the damage that could have been caused 20 years ago by adopting a key escrow system would today be even more severe — causing unanticipated and hard-to-detect security flaws that could be exploited by hackers.[38]

## 3. Authenticating a Person, Device, or Computer

Many critical services and features available on the Internet only work securely if the service provider can authenticate the person, device, or computer seeking access. Authentication is the process of ensuring both ends of the connection are who they say they are. Not only do you need to authenticate who you are when you log onto a website or sign into a bank account, but many of the most powerful features of the web are enabled when you can protect your password from ever being stolen, but still log into accounts.

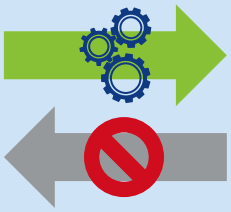
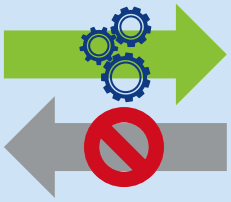
### *Hashing to Protect Passwords*

One important encryption-enabled technology is called hashing. When people say passwords are encrypted, they are generally referring to hashing — a commonly used technique for protecting your password if a website is ever hacked and the cybercriminals get access to the master password file. Rather than storing a file on the server that contains a master plaintext list of every user's password, passwords instead are run through a hashing process so that a hacker could only obtain what looks like a random set of digits. Your actual password never needs to be stored on the server, and thus can never be directly breached.

Hashing transforms the password (or other text) into a fixed-length string of random-looking data by relying on two important properties. First, the same input password (or other text) will always produce the same hash string. This feature means that a given password will always produce the same exact hash, enabling the website or cloud providers to easily determine if the hash matches a previously stored hash. Second, it is impossible to reverse the operation and use the hash string to reproduce the original password. A one-way hashing algorithm is the mathematical equivalent of scrambling eggs: it is quite easy to mix, cook, and eat scrambled eggs, but impossible to reconstruct the original egg after it has been scrambled, cooked, and eaten.

Hashing is not only used for passwords, but also is used to verify that a file has not been corrupted or infected with a virus, and is used

### A GLIMPSE INTO HASHING

| Cleartext | Hashing | SHA-256 digest |
|---|---|---|
| Example: *"MyGreatPassword!"* |  | 46FC913D82F997256DC6E91CF80FABA0<br>83D49F6B836000A1C8EC15668B91A338 |
| Example: *"Hashing's unique one-way mathematical properties help secure your passwords online. A hash creates the same size key regardless of the length of the text."* |  | B50362640C9B447A0B3FB08F08550674<br>2F8EAC9045FFD2D960FC14A1B34AF5D2 |

to generate unique keys to speed up the process of searching through large databases.

The process behind a hashing function takes advantage of unique mathematical properties. For example, the folding method converts the password into numbers, divides it into several parts, adds the parts together, and then uses the last four digits as the hashed key. The digit remainder method, using modulo arithmetic, simply takes an item and divides it by the size of the hash key, returning the remainder as its hash value for a given position in a hash key. Common hashing algorithms include the Secure Hash Algorithm (SHA) variants SHA-1, SHA-2, and SHA-3, as well as MD5.

### *Authentication*

To enable websites and Internet-connected devices to interact with one another without impeding security, there are important encryption-enabled technologies that protect the data your online service might expose. For example, third-party authentication technologies that allow Single Sign On have been widely adopted to enable users to keep a single repository of user names and passwords that can be used across several applications. Technologies like OpenID, SAML, and OAuth allow users to give authorization or enable authentication to other websites or web-enabled devices without having to share a private password with the third party. OpenID technology, for example, commonly allows users to log into third-party websites using their Microsoft, Google, PayPal, Yahoo!, or Facebook passwords, without requiring the third party to store your private password. This is not only a critical security-enhancing technology used today, but standards like oAuth will become increasingly important for authenticating and enabling the Internet of Things where users need to give permission so devices can talk and interact with each other.

## Staying One Step Ahead

Security researchers often are only one step ahead of the fast-moving cyber-threat landscape. Adversaries are working around the clock, and around the globe, seeking to mercilessly take advantage of even minor design flaws. Over time, researchers have reported that many forms of once-unbreakable encryption standards now have become almost trivial to break.

Given the widespread reliance on encryption for enabling vast parts of our economy and critical infrastructure, it's important that innovators be able to continue to push the envelope in finding newer and stronger ways to protect digital security, and optimize individual privacy. Their ability to improve and combine multiple forms of strong encryption and authentication is essential for continuing to stay at least one step ahead of emerging threats and actors — in the process ensuring the security at the heart of the digital economy, protecting our critical infrastructure and national security, and protecting our most personal digital online secrets. Weakening any part of the system can open up potentially disastrous opportunities for bad actors to undermine our very way of life.

# The Current Policy Debate

The various forms of encryption technologies described above each are built upon common trustworthy standards and algorithms that are used and trusted around the globe. In order to ensure law enforcement access, some have recently proposed solutions that would limit the use of security technologies, require flaws to be built in to technology, or dictate design and capabilities by requiring systems to use or design master encryption keys.

***Cryptographers warn that it is impossible to weaken encryption without strengthening the hands of hackers and foreign adversaries.***

Unfortunately, such proposals would actually undermine the effectiveness of the security tools necessary to keep information safe and secure, and risk undermining the security of all electronic communications and digitally stored information.

## *Here's Why*

Some well-intentioned proposals would simplistically require technology companies to decrypt data on demand regardless of whether the companies have access to the key. Such requirements could force companies who today make technology needed for data security to create solutions that are weak enough to break (making it more likely bad actors could break it, too). Other common suggestions for improving government access to encrypted information involve weakening or mandating weak encryption standards, as happened in the original DES encryption standards.[39] By definition, that weakens the security of all products that rely upon those standards, while increasing the possibility that bad actors would exploit the technology.

Others suggest forcing providers to distribute illegitimate public keys in order to implement what is essentially a man-in-the-middle-attack, or requiring providers to adopt some form of mandatory key escrow system whereby somebody or some entity is a "master" key escrow holder. Such an approach appears to stem from the belief that there must be some other way to force players who don't have the keys to provide un-encrypted access to information, without weakening the strong encryption built into products and services. Yet such escrow solutions, eventually rejected by policymakers in the 1990s as insecure, would create a new single point of attack to be exploited, create new risks from possible data breaches when all the keys are stored together, and take from individuals the power to secure their own data.

For these and other reasons, a group of leading cryptographers has warned that various efforts to weaken technology in order to give law enforcement access to encrypted communications will inevitably be used by sophisticated hackers and foreign adversaries.[40] Cryptographers warn that it is impossible to weaken encryption without strengthening the hands of hackers and foreign adversaries. It is one of the reasons why more and more technologists, policymakers, and innovators are coming to reject suggestions to ban end-to-end encryption, or in some way mandate weak encryption.[41] A broader, open dialogue on the issue is needed.

# Conclusion

Although encryption can seem mathematically and technology complex, its story is quite simple: **the widespread use of strong encryption is enabling many consumer benefits, helping drive our economy, and protecting our nation's critical infrastructure and security.**

**Learn more at bsa.org/encryptionmatters.**

[1] More than 70 percent of Americans now take advantage of cloud-based apps. The popularity of cloud services has taken off in part because the data can be protected by encryption when it's in transit to and from the cloud, and also when it's stored in the cloud at rest. At rest, some cloud providers use AES-256 to encrypt the data on their side; others let the user do the encrypting and decrypting. Schools often deploy encrypted cloud services to protect the confidentiality of student records and comply with the Family Educational Rights and Privacy Act (FERPA). See Rich Miller, "Pew: 69 Percent of Americans Use Cloud Apps," *Data Center Knowledge*, available at http://www.datacenterknowledge.com/archives/2008/09/12/pew-data-shows-solid-uptake-for-cloud-apps/.

[2] In order to enable employees to work anytime, anywhere, over virtually any devices, Virtual Private Networks (VPN) have become a mission-critical business technology by enabling a secure encrypted pipe to tunnel through the public Internet in order to protect the communication between a laptop and a work server. VPNs can use various different encryption technologies including Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), Secure Shell (SSH) or Secure Socket Tunneling Protocol (SSTP), all of which encapsulate IP packets inside an encrypted packet.

[3] Encryption protects billions of daily e-mails from prying eyes while in transit. In addition to the secure HTTPS connection often activated by default when accessing a web based e-mail service, if you use an e-mail client or other service to access your cloud based e-mail account, consumers generally have the option to use SSL/TLS encryption to protect e-mails in transit. Some people also encrypt the contents of their e-mail with encryption tools like PGP.

[4] With some of our most sensitive moments, business dealings, and confidential information now regularly shared over instant messaging services, many messaging services, including iMessage, Blackberry messenger, Yahoo! Messenger, Facebook chat, FaceTime, and WhatsApp, use various forms of encryption to protect the data. See Wikipedia, "Comparison of Instant Messaging Clients," available at https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients#Secure_messengers.

[5] Surveys show consumers want the ability to protect their most sensitive information, including location data. Federal agencies have warned that protecting consumer location data is especially important for protecting consumers against physical security threats, stalkers, and identity theft. See *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not Be Clear to Consumers*, Testimony Before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate (June 4, 2014), available at http://gao.gov/assets/670/663787.pdf.

[6] When you visit a public place like a restaurant, coffee shop, or airport, a secure encrypted Wi-Fi connection between your device and the router can help prevent others from intercepting your credentials or hijacking your session. Wi-Fi routers and laptops can take advantage of WPA2 encryption, which can take advantage of AES algorithms to protect digital data. This security is also important at home where, according to one survey of US households, 88 percent of Americans say they are uncomfortable with unsecured Wi-Fi that enables unauthorized neighbors or passersby to access their home network. See Neil J. Rubenking, "Survey Shows Many Home Networks Are Insecure," *PCmag.com*, available at http://securitywatch.pcmag.com/hacking/329237-survey-shows-many-home-networks-are-insecure.

[7] As of April 2015, 29 percent of all Internet traffic in North America was encrypted. See "Global Internet Phenomena Spotlight," *Sandvine*, April 8, 2015, available at https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

[8] To secure the physical credit card transactions of the estimated 1.2 billion debit and credit cards in circulation among the 335 million people who live in the US, in October 2015 the US made the shift to credit cards that each contain a unique encrypted token that allows the bank to decrypt in and verify your account to authorize payment, and prevent the cloning of cards. See Matt Hamblen, "FAQs: What You Need to Know About Chip-Embedded Credit Cards," *ComputerWorld*, available at http://www.computerworld.com/article/2960791/financial-it/faq-what-you-need-to-know-about-chip-embedded-credit-cards.html.

[9] Smartwatches are wirelessly connected to smartphones using Bluetooth, which uses AES-CCM 128-bit encryption to ensure that your wireless connection is secure. To the extent that you use smartphone apps that are personalized to you and link to the Internet (like a payment app), they are also likely to use various forms of encryption to protect your password, as well as the data in motion. See https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx.

[10] 50 percent of Americans use an ATM at least eight times per month. From the moment they type in their pin number, the ATM transaction is processed and protected electronically using AES encryption. See David Dunning, "What Encryption Is Used on an ATM Machine?," *eHow*, available at http://www.ehow.com/info_11369995_encryption-used-atm-machine.html and Jeff Sipes, "43 Fun Facts About ATMs," *Activerain*, available at http://activerain.com/blogsview/4428147/43-fun-facts-about-atm-machines-

[11] With more than 56 million Americans already having accessed their health records online, more and more Americans are expecting and demanding online access to health data. To protect the privacy and security of sensitive medical data, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires "A covered entity must, in accordance with §164.306… Implement a mechanism to encrypt and decrypt electronic protected health information." (45 CFR §164.312(a)(2)(iv)). See "56 Million and Growing — Survey Confirms People Want Online Access to Their Health Records," *ViewMyHealthRecords.com*, available at https://www.viewmyhealthrecords.com/56-million-and-growing-%E2%80%93-survey-confirms-people-want-online-access-their-health-records.

[12] Beyond the device encryption that protects the personal information on a smartphone with a passcode, to protect the privacy of the three billion cellular voice calls made every day in the US, cellphones for decades have used various authentication and encryption technologies to prevent your call from being inadvertently recorded or intercepted. For example, 3G phones use Authentication and Key Agreement (AKA) protocol for the tower connection. Call encryption in 3G uses a proprietary block cipher called KASUMI. See Wikipedia, "Authentication and Key Agreement (Protocol)," available at https://en.wikipedia.org/wiki/Authentication_and_Key_Agreement_(protocol) and Wikipedia, "KASUMI," available at https://en.wikipedia.org/wiki/KASUMI.

[13] The 61 percent of Internet users who bank online have their information protected by encryption. Online sessions between the browser and the bank server are protected by Transport Layer Security (TLS). The connection between the bank and the rest of the banking system is also encrypted. Because it's secure, consumer online and mobile banking is projected to double from $2.5 trillion a year in 2014, to nearly $5 trillion by 2019. See Susannah Fox, "51% of U.S. Adults Bank Online," Pew Research Center, available at http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/ and David Bannister, "Online Transactions to Touch $5 Trillion in 4 Years' Time," Banking Technology, available at http://www.bankingtech.com/228542/online-transactions-to-touch-5-trillion-in-four-years-time/.

[14] 96 percent of Americans are paid electronically via direct deposit, which is routed securely between banks by the Automated Clearing House (ACH) system, which is a secure, private network that connects banks to one another by way of the Federal Reserve Board or other ACH operators. This network enables electronic payments, such as automatic payroll deposits and debit card purchases, to be handled and processed. See Maria Trombly, "Automated Clearing House," *Computerworld*, available at http://www.computerworld.com/article/2591833/app-development/automated-clearing-house.html; NACHA, "What Is ACH? Quick Facts About the Automated Clearing House (ACH) Network," available at https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network; Lisa Hephner, "ACH Security Requirements for Merchants," available at https://paysimple.com/blog/ach-security-requirements-for-merchants/; and SPMI, "96 Percent of Americans Are Paid Electronically Via Direct Deposit," available at https://myhrprofessionals.com/2013/09/25/96-percent-of-americans-paid-electronically-via-direct-deposit/.

[15] Encryption is the catalyst that enables US consumers to securely buy more than $330 billion a year in online goods and services. Every time you enter your credit card number on the Internet, encryption springs into action to protect it. Not only does SSL encryption protect the connection between your browser and the server, but then the Payment Card Industry Data Security Standard (PCI DSS) kicks in — it's an information security standard for businesses that handle, process, and store credit cards. See Matt Lindner, "Online Sales Will Reach $523 Billion by 2020 in the U.S.," *Internet Retailer*, available at https://www.internetretailer.com/2016/01/29/online-sales-will-reach-523-billion-2020-us.

[16] Many connected devices now take advantage of encryption to protect their security. For example, the Nest Thermostat and its app connect to the Nest cloud service using AES 128-bit encryption and Transport Layer Security (TLS). See Nest, "Keeping Data Safe at Nest," available at https://nest.com/security/.

[17] Consumers spent about $1.3 billion ordering movies and other video-on-demand from their pay TV services. These providers protect against intellectual property and service theft by encrypting premium channels and sometimes even basic channels so that they can't be viewed without a cable box. Encryption also enables consumers to rent videos on-demand, and the service provider to protect the information about what consumers are renting as required under the Video Privacy Protection Act. See "Cable Continues Dominance of On-Demand Movie Sales," *USA Today*, available at http://www.usatoday.com/story/tech/personal/2013/03/04/telecom-tv-movie-sales/1961869/.

[18] Many online services take advantage of third-party authentication technologies that enable Single Sign. That way, when someone wants to use an app like TwitPic or Tweetgif to post a funny animated GIF to their Twitter account, they use encryption. In the background, Twitter uses authentication technology to give the application access to your Twitter account without you every having to provide the application access to your username and password directly.

[19] In order to protect intellectual property, on-demand music services like Spotify, Rhapsody, Google Play Music, Beats Music, etc. encrypt streams as well as music tracks that users download for "offline listening." As a result, more than 11 million people now subscribe to online music services and listen to billions of hours a month of music. See Bill Rosenblatt, "The Myth of DRM-Free Music," *Copyright and Technology*, available at http://copyrightandtechnology.com/2015/05/31/the-myth-of-drm-free-music/.

[20] One economic assessment found profound growth enabled by encryption. For consumers, it calculated annual consumer surplus resulting from the use of ICT services employing encryption was $29.40 per user. See Ryan Hagemann and Josh Hampson, "Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption," Niskanen Center, available at https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

[21] About 55 percent of compromised records in the health care sector are the result of a failure to encrypt data, according to a California Data Breach Report. See "Health Care Needs to Do a Better Job Encrypting Data: Report," *Wall Street Journal* (February 22, 2016), available at http://blogs.wsj.com/cio/2016/02/22/health-care-needs-to-do-a-better-job-encrypting-data-report/.

[22] Encrypted analysis of data in the cloud would allow secure access to sensitive information and the processing of DNA sequence data to speed up discovery of disease-linked gene variants. See Erika Check Hayden, "Extreme Cryptography Paves Way to Personalized Medicine," *Nature.com*, available at http://www.nature.com/news/extreme-cryptography-paves-way-to-personalized-medicine-1.17174.

[23] A lack of encryption created a security flaw that enabled hackers to unlock car doors. But connected cars could have as big of an effect on safety as seatbelts — reducing injuries and fatalities by as much as 50 percent. See Jerry Hirsch, "Hackers Can Now Hitch a Ride on Car Computers," *Los Angeles Times* (September 13, 2015), available at http://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html and Claire Cain Miller, "If Robots Drove, How Much Safer Would Roads Be?" *New York Times* (June 10, 2014), available at http://www.nytimes.com/2014/06/10/upshot/if-robots-drove-how-much-safer-would-roads-be.html?ref=technology&_r=0.

[24] Darlene Superville, "Obama Wants $4 Billion to Help Students Learn Computer Science, Programming," *Orange County Register* (January 31, 2016), available at http://www.ocregister.com/articles/science-702194-computer-obama.html.

[25] The National Security Agency (NSA) has played a key role in developing many forms of strong encryption in order to protect our national security, whereas NIST works to create the strongest possible encryption standards for the US government and industry at large. See Wikipedia, "NSA Encryption Systems," available at https://en.wikipedia.org/wiki/NSA_encryption_systems; Edwin Key, "US Drone Transmissions Are Not as Secure as We Think," *UberGizmo.com*, available at http://www.ubergizmo.com/2012/10/us-drone-transmissions-are-not-as-secure-as-we-think/; and Gail Porter, "Cryptographic Standards Statement," NIST Office of the Director, Press Release (September 10, 2013), available at http://www.nist.gov/director/cybersecuritystatement-091013.cfm.

[26] Jeff Hudson, "Smart Grids: Digital Certificates and Encryption Play Key Role in Security," *Security Week* (October 18, 2012), available at http://www.securityweek.com/smart-grids-digital-certificates-and-encryption-play-key-role-security.

[27] US Department of Homeland Security, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies" (October 2009), available at https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf.

[28] American Water Works Association, "Process Control System Security Guidance for the Water Sector," available at http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf.

[29] International Atomic Energy Agency, "Computer Security at Nuclear Facilities," available at http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.

[30] Aaron Cooper, "Report: Air Traffic Control System Vulnerable to Cyberattack," available at http://www.cnn.com/2015/03/02/politics/cyberattack-faa-air-traffic-control-hacking/.

[31] As many as 410 million people worldwide are using private browsers, VPNs, and other software to browse the internet in anonymity, according to research firm Globalwebindex. See Chris Smith, "Seriously Dark Traffic: 500 Mil. People Globally Hide Their IP Addresses," *Digiday* (November 18, 2014), available at http://digiday.com/publishers/vpn-hide-ip-address-distort-analytics/.

[32] Wikipedia, "40-Bit Encryption," available at https://en.wikipedia.org/wiki/40-bit_encryption.

[33] Wikipedia, "EFF DES Cracker," available at https://en.wikipedia.org/wiki/EFF_DES_cracker.

[34] 40-bit encryption was common in software released before 1999, when algorithms with larger key lengths could not legally be exported from the United States without a case-by-case license. See Wikipedia, "40-Bit Encryption," available at https://en.wikipedia.org/wiki/40-bit_encryption.

[35] By 1997, advances in computing technology had rendered 40-bit encryption dangerously weak and export limits commercially obsolete. See Ellen Fitzmaurice and Kevin Tamaki, "Decoding the Encryption Debate," *Los Angeles Times* (June 1, 1997), available at http://articles.latimes.com/1997-06-01/local/me-64597_1_encryption-debate.

[36] For example, when a company escrows keys for when BitLocker is used to secure corporate data at rest on corporate laptops.

[37] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard" (August 20, 1994), available at http://www.crypto.com/papers/eesproto.pdf.

[38] Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Computer Science and Artificial Intelligence Laboratory Technical Report (Cambridge, MA: Massachusetts Institute of Technology, July 6, 2015), available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[39] In 1976, after consultation with the NSA, the National Bureau of Standards adopted a modified standard that was weakened against brute force attacks. The relatively short key length led to easy breakage, and as a result has long been considered an unsafe form of encryption. See Wikipedia, "Data Encryption Standard," available at https://en.wikipedia.org/wiki/Data_Encryption_Standard.

[40] Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Computer Science and Artificial Intelligence Laboratory Technical Report (Cambridge, MA: Massachusetts Institute of Technology, July 6, 2015), available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[41] As President Obama said, "There's no scenario in which we don't want really strong encryption." See Liz Gannes, "Obama: The Re/Code Interview," available at http://recode.net/2015/02/13/obama-theres-no-scenario-in-which-we-dont-want-really-strong-encryption/.