Beyond Secrets: The Consumer Stake in the Encryption Debate

December 21, 2017

ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

Consumer Reports' donors and philanthropic partners play a critical role in our efforts to promote consumer interests in relation to privacy, security, and data practices. We gratefully acknowledge the William and Flora Hewlett Foundation for its support of this report and related communications.
Consumers Union, the policy and mobilization division of Consumer Reports, partnered with Upturn, a nonprofit organization based in Washington, D.C., working at the intersection of social justice and technology, to write this report on consumers' stake in the encryption debate.

Introduction

For more than 20 years, industry and government have tangled over the issue of commercial data encryption—a digital tool that scrambles messages and other data to ensure that they cannot be accessed by anyone for whom they are not intended. In the early days of the web, the debate focused on such issues as whether it would be safe to export encryption technology outside the United States.[1] As technology and the use of encryption have evolved, however, so has the debate and encryption's relevance to the daily life of the average American consumer.

Today's debate is generally framed as a struggle between civil liberties and national security. Civil liberties groups generally support encryption in order to protect personal data and communications from intrusion and misuse by hackers, and from unwarranted access by the government.[2] Many corporations, too, have supported strong encryption in order to promote free expression and engender trust in their services.[3]

By contrast, government officials worry that commercial encryption tools shield criminals and terrorists from detection and prosecution by law enforcement. As a result, some of these officials have called for "backdoors" or "exceptional access" to encrypted data to allow law enforcement to gain access to secure communications when needed.[4]

We maintain that the discussion on the question of whether or not personal communications should be protected fails to fully recognize the many other benefits of strong encryption. The purpose of this paper is to reveal and review the countless ways that strong encryption supports and improves the everyday lives of U.S. consumers and the daily functioning of the marketplace. By ensuring the confidentiality, integrity, and authenticity of data transmissions, encryption provides essential safeguards across many aspects of our lives, including, but not limited to:

- Consumers' health records, medical devices, and virtual healthcare visits;
- Personal banking transactions, online credit card use, and mobile payments;
- Software updates to our laptops, phones, and other devices;

---

[1] Jack Karsten & Darrell M. West, *A Brief History of U.S. Encryption Policy*, BROOKINGS INST. (Apr. 19, 2016), https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy.

[2] *Coalition Urge Nations to Defend Strong Encryption*, ELEC. PRIVACY INFO. CTR. (July 10, 2017), https://epic.org/2017/07/epic-coalition-urge-nations-to.html; Danny Yadron, *Facebook and Twitter Back Apple in Phone Encryption Battle with FBI*, THE GUARDIAN (Feb. 18, 2016), https://www.theguardian.com/technology/2016/feb/18/apple-fbi-encryption-battle-iphone-facebook-twitter-san-bernardino-shooting.

[3] *See, e.g.*, *Encryption: Helping to Protect Data at Rest and Data in Transit*, MICROSOFT, https://www.microsoft.com/en-us/trustcenter/security/encryption; Letter from Apple to its customers, APPLE (Feb. 16, 2016) *available at* https://www.apple.com/customer-letter; Brian Barrett, *Don't Let Wikileaks Scare You Off of Signal and Other Encrypted Chat Apps*, WIRED (Mar. 7, 2017), https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps.

[4] *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, CTR. FOR DEMOCRACY & TECH. (Mar. 3, 2016), https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance; *Encryption and the "Going Dark" Debate*, CONG. RESEARCH SERV. (July 20, 2016), 13-14, *available at* https://epic.org/crs/R44481.pdf.

- Billions of connected devices, including "smart" home appliances and the software in our cars;
- Emergency broadcast systems and other public communications channels;
- Nationally important infrastructure, including air traffic systems; and
- Emails, text messages, voice calls, and social media.

These basic, essential functions all rely on encryption, and the consequences to the lives of consumers if they were compromised would be extraordinary. In some areas—for example, the availability of telehealth in rural communities or the prevention of identity theft—such compromise could have a particularly adverse impact on the most vulnerable consumers. In other areas—for example, the use of medical devices in hospitals—the use of encryption is essential to patient safety and should be strongly encouraged to foster more widespread adoption. As policymakers consider the boundaries of encryption and government access to encrypted data, the many important consumer benefits that encryption provides need to be part of the conversation.

Cryptography: The Crucial Ingredient

Modern cryptography—the science of secret communications—sits at the core of consumers' digital security. Through decades of research, mathematicians and computer scientists have developed the basic building blocks that allow people to communicate securely online. Encryption and digital signatures (described below) are common applications of the principles of cryptography. These building blocks of cryptography are extremely robust: Even if all of the world's computers simultaneously attempted to break the best modern encryption, they would be left crunching numbers for a billion years.[5] Today, consumers are more reliant on this cryptographic foundation than ever before.

Encryption and digital signatures are two sides of the same coin: They share a common cryptographic lineage and rely on the same mathematical building blocks. More importantly, they work *together* to provide strong digital security.

Encryption and digital signatures can be likened to the envelopes and wax seals of the pre-digital age. The envelope—encryption—provides confidentiality for its contents. The wax seal—digital signatures—allows the recipient to both identify the sender *and* verify that the contents of the envelope haven't been tampered with. Envelopes and wax seals were necessary in their day, and they worked in tandem to provide for secure communications. If one or the other was compromised—if the envelope was ripped or the wax seal was invalid or tampered with—the recipient would have reason to question the legitimacy of the message. The same is true for encryption and digital signatures today. Weakening one of these functions undermines the credibility of any communications that purport to be secure.

[5] Mohit Arora, *How Secure Is AES Against Brute Force Attacks?*, EE TIMES (May 7, 2012), http://www.eetimes.com/document.asp?doc_id=1279619.

It is also important to remember that cryptographic functions do not just protect traditional, person-to-person communications, such as voice- and text-based messages. They also secure and validate the transmission of all kinds of data, including financial transactions, web traffic patterns, GPS signals, and software updates that flow over mobile and internet connections.[6] When we refer to "messages" and "communications," then, we mean everything that happens on the internet, from online banking activity to route-mapping apps on a person's phone.

How encryption works

At its most basic, digital cryptography is nothing more than two people sharing a common technique to scramble and unscramble messages. The benefit of encryption is that it delivers *confidentiality* so that even if someone intercepts one of these messages, that person cannot unscramble it. As an example, one very primitive technique known as ROT-13 simply replaces each letter in the alphabet with the letter 13 letters after (or before) it in the alphabet. Thus, the message "MEET AT MY HOUSE AT EIGHT" becomes "ZRRG NG ZL UBHFR NG RVTUG" using ROT-13. This encrypted message would be unintelligible to a person who saw it written on a scrap of paper, but a person who knew to use ROT-13 to decrypt the message would be able to interpret the message with a little counting. This type of encryption is known as "symmetric-key encryption," because the sender and the recipient use the same key to encrypt and decrypt the message. Any person who intercepts or otherwise receives encrypted data but does not possess the key should not be able to read it.[7]

The primary disadvantage of symmetric-key encryption is that both communicating parties need to know the secret key in advance. This presents a challenge for strangers who wish to communicate secretly, or for individuals to communicate securely with a business, such as on a public website. To solve for this problem, cryptographers developed "asymmetric encryption" or "public-key encryption." With this method, a person has a public encryption key that is publicly

[6] Ryan Browne, *IBM Unveils New Mainframe Capable of Running More Than 12 Billion Encrypted Transactions a Day*, CNBC (July 17, 2017), https://www.cnbc.com/2017/07/17/ibm-unveils-new-mainframe-capable-of-running-more-than-12-billion-encrypted-transactions-a-day.html (on financial transactions); Klint Finley, *Half the Web Is Now Encrypted. That Makes Everyone Safer*, WIRED (Jan. 30, 2017), https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer (on web traffic); Mark L. Psiaki and Todd E. Humpreys, *Protecting GPS From Spoofers Is Critical to the Future of Navigation*, IEEE SPECTRUM (July 29, 2016), https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation (on GPS); Paul Rubens, *6 Tips for Developing Secure IoT Apps*, ESEC. PLANET (Feb. 26, 2015), http://www.esecurityplanet.com/network-security/6-tips-for-developing-secure-iot-apps.html.

[7] Of course, an attacker could try to guess the key or attempt to try every possible key in order to decipher the data into something intelligible. Designers of cryptographic systems must craft their systems to resist such *brute force* attacks, meaning that attempting to decrypt the data with every possible key would be too costly or time-consuming. Alternatively, an attacker could try to discover a flaw in the underlying algorithm that could allow the attacker to determine the value of the key from other information. As computers become more powerful, capable of performing faster and faster calculations, new encryption algorithms are constantly being developed or improved to account for attackers' ever-increasing ability to perform more and more guesses and to discover potential vulnerabilities in the algorithms themselves.

available to the world, as well as a private encryption key that is not shared. Anyone wanting to send that person an encrypted message can encrypt the message using the public key. However, that message cannot be decrypted with that public key—it can be decrypted only with the private key. This public-key architecture is the foundation for most web and internet encryption, enabling consumers to have private conversations with any other person or business around the world.[8]

The encryption described here is encryption "in transit," because it protects data as it traverses from Point A to Point B. Data can also be encrypted "at rest" on digital storage. In this case, only one key is needed (say, a password) because the person who encrypts the data is typically the one who will also decrypt the data. In this way, encryption can be used to protect stored data in a corporate or government database so that it cannot be read in the event of a data breach. Unfortunately, many databases are left unprotected, as the many recent high-profile data breaches have demonstrated.

How digital signatures work

There is more to security than confidentiality. It is equally important for consumers to know to whom they are talking over a network, and whether a message has been tampered with prior to delivery.

Cryptography can address these needs by helping to create digital signatures, which guarantee the authenticity and integrity of a message. By digitally signing each message, two people can be sure that they are actually talking to each other, rather than exchanging messages with an imposter. They can also verify that the messages they receive are exactly as they were originally sent and have not been modified while in transit.

In public-key cryptography, digital signatures work in essentially the opposite manner as encryption: A hash[9] is created of the message, then that hash is encrypted using the sender's private key, such that it can be decrypted only with the sender's public key. Both the hash and the encrypted hash are then sent. Anyone can decrypt the hash using the public key, but only someone in possession of the private key can encrypt the data in the first place. If after decryption the two hashes do not match, the receiver knows that either the message was

[8] In practice, web encryption is more complicated than this; often the public key encryption is primarily used to transmit a symmetric key (and other communication parameters) that will be used to encrypt the rest of the communication. However, it is accurate to say that public key encryption is used to *initiate* encrypted communication between disparate parties over the internet.

[9] A cryptographic hash is a one-way mathematical function that converts any amount of data into a unique, fixed-length string. The string should bear no clear link to the original text, and the hashing algorithm is designed to make reverse engineering the original text from the string to be unreasonably difficult. Every time that data is hashed, it generates the same exact string. And hashing algorithms (such as MD5 or SHA-256) are designed to avoid *collision*, or different original values generating the same hash result. For example, the MD5 hash of the full text of the Declaration of Independence is "5892487d6cd85159b5cce011a5588c94"; ideally, no other input should result in that same result.

tampered with or the person encrypting the message did not possess the putative sender's private key.[10]

The complementary functions of encryption and digital signatures often operate behind the scenes: In many cases, consumers need not do anything to reap the benefits of cryptography, because the designers of the products they use have already built in strong cryptographic features. The invisible and automatic nature of cryptography also means that consumers are generally unaware of it, and are thus unlikely to realize its value or express support for it in the marketplace.

How 'backdoors' work

While cryptography has clear privacy and other consumer benefits, it does place significant limitations on law enforcement and intelligence, which lack the capacity to decipher encrypted communications and content. For example, in the course of investigating the 2015 mass shooting in San Bernardino, Calif., the Federal Bureau of Investigation sought to investigate the contents of the shooter's phone in order to determine whether others were involved in planning the attack. However, the phone was encrypted and the police did not possess the password to the device; ultimately, they went to court to compel Apple to assist them in decrypting the phone's contents.[11]

In order to give the government the capacity to view encrypted content when necessary, various proposals have been brought forward in recent years to mandate that the design of cryptographic systems allows for government access; these proposals are loosely referred to as mandated backdoors for encryption. As one example, some have proposed "key escrow" as one backdoor approach: Copies of private encryption keys would be required to be stored in escrow, which the government could petition to gain access to in order to decrypt communications necessary for legitimate law enforcement or intelligence purposes with appropriate court supervision.[12]

While these proposals would give the government greater ability to access encrypted communications, that access would come at great cost to consumers and the services and

[10] Digital signatures can confirm that a message came from someone in possession of a certain private key; by themselves, they do not necessarily tell you anything about who is behind a particular public and private key pair. To address this, companies known as *certificate authorities* issue digital certificates to websites containing certain identifying information about the website along with the site's public key. Certificate authorities offer different types of certificates depending on how much verification is done to authenticate the identity of a site owner. Banks and other financial institutions often opt for the highest level of verification in order to demonstrate to users that they are in fact responsible for specific financial websites. Other sites that process less sensitive data may prefer lower validation—or even self-signed—digital certificates (though browsers may indicate that those sites offer a lesser degree of reliability).

[11] The FBI's application was subsequently withdrawn after it found a third-party company that was able to decrypt the device without either the device owner's password or Apple's assistance. *See* Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0.

[12] *Key Escrow*, ELEC. PRIVACY INFO. CTR. (Apr. 14, 1998), https://epic.org/crypto/key_escrow.

infrastructure they have come to rely upon: Mandating backdoors weakens the underlying security properties of encryption and increases the chance that encrypted data and devices will be accessed by malicious actors—not just by law enforcement. Key escrow, for example, creates a centralized repository of private keys for criminals to attack—or rather repositories, because multiple law enforcement entities around the world may require their own access system. If such a database were compromised, any user-encrypted communication could also be compromised, and the user's identity could be forged to falsely authenticate bogus communications. Mandating backdoors also introduces additional complexity to every cryptographic system, increasing the chances of vulnerabilities that could be exploited.[13]

How Consumers Benefit From Encryption

As described above, cryptography provides the foundation for the secure transmission of data over the internet, which, in turn, deeply affects people across many different domains of their lives. Any debate about whether to employ—or compromise—encryption must weigh the considerable benefits that consumers enjoy every day as a result of encryption technology.

Cryptography is essential for secure online communication, and consumers spend big swaths of their lives online. Encryption and digital signatures are what enable us to trust the safety and credibility of the messages and data we send and receive all day, and every day, as we use and rely on the internet for our basic functioning.[14]

Today, more than 84 percent of American adults use the internet, including more than 95 percent of those ages 18 to 29.[15] Seventy-seven percent of Americans own smartphones, which most use for online banking, accessing employment and health information, social networking, and driving directions.[16] About 80 percent of Americans shop online.[17] The emerging "Internet of Things" (IoT)—a label that covers everything from digital video recorders to home routers to "smart" toasters—is expected to balloon to approximately 20.4 billion connected devices by 2020.[18] The majority of the connected devices in use will be in the hands of consumers.[19]

---

[13] For a more thorough discussion of the potential threats caused by mandated backdoors, *see* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, (July 7, 2015), https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

[14] It is important to note that even if a communication is encrypted, it may still be susceptible to interception. For example, if a device is compromised with malware, encryption will not prevent an attacker from eavesdropping on a conversation because the contents can be observed on the device *after* decryption. And even if a communication is encrypted, the implementation of the encryption may be flawed, allowing attackers to access information by taking advantage of inadvertent vulnerabilities. However, properly implemented encryption protects against many common threats. *See Experts in Support*, *infra* note 73.

[15] Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RESEARCH CTR. (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015.

[16] *Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile.

[17] Aaron Smith and Monica Anderson, *Online Shopping and E-Commerce*, PEW RESEARCH CTR. (Dec. 19, 2016), http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce.

[18] *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, GARTNER (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917.

To consumers, the most familiar indicator of cryptography at work is the little green "lock" icon that appears in our web browsers at the start of many URLs, or web addresses. HTTPS—the secure version of the Hypertext Transfer Protocol that underpins the web—is one of the most important and ubiquitous digital security tools in the world today. Every time consumers log on to their bank account to pay credit card bills, apply for healthcare and other public benefits online, upload a photo of their family to a social network, or make a purchase on a mobile app, they are relying on HTTPS.

Importantly, HTTPS is not limited to websites; it also secures connections for hundreds of thousands of mobile apps, cloud software programs, point-of-sale systems, and other applications that drive economic activity and animate society.

HTTPS exemplifies all of cryptography's best features. It makes it difficult for hackers, third-party companies, and governments to monitor what consumers do online. It validates that a consumer's computer is communicating with the website it intended to reach, and guarantees the integrity of the data sent between the computer and a website. And it is seamless from the user's point of view; after a consumer clicks on a link beginning with HTTPS://, the power of cryptography springs to life. Behind the scenes, the web browser uses encryption and digital signatures to create a secured, trusted communication channel. Consumers only need to see the lock icon to know they are browsing securely, that the connection is private, and that it is safe to enter personal details through an online form or to send credit card information to a retailer.[20]

The use of HTTPS is spreading rapidly. Today, all banking and e-commerce websites routinely use HTTPS, protecting hundreds of millions of consumers from financial fraud. HTTPS has become standard for social media sites, email services, and other popular communication platforms. And a 2015 White House policy requires all publicly accessible federal websites and web services to employ HTTPS, noting that users of these services deserve the same protection they get from the private sector.[21] Below, we discuss more in depth many specific examples of how consumers benefit from encryption.

Protecting consumers' health

Healthcare is primed for transformation as new technologies promise to reduce the cost of care and improve patient outcomes. However, many of the drivers of these benefits—such as the digitization and sharing of medical information and the increased use of connected medical devices and remote access to doctors—also demand sound digital security to protect patients'

[19] "The consumer segment is the largest user of connected things, with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use," *Id*.
[20] As noted previously (*supra* notes 7, 8), encryption does not protect against all threats; however, it does provide substantial assurance to consumers that their communications will not be intercepted en route to their destination.
[21] Tony Scott, *HTTPS-Everywhere for Government*, THE WHITE HOUSE, PRESIDENT BARACK OBAMA (June 8, 2015), https://obamawhitehouse.archives.gov/blog/2015/06/08/https-everywhere-government.

health and health privacy.

Medical data

Digitization of medical information has raised the stakes for robust information security in healthcare. Starting in 2014, public and private healthcare providers were required by the American Recovery and Reinvestment Act of 2009 to "demonstrate meaningful use of electronic medical records."[22] In support of this requirement, proponents cited the potential for improving the quality, efficiency, and convenience of healthcare as doctors would be able to instantly access health records across providers and make faster decisions while avoiding risks.[23] But this requirement led to an unexpected skyrocketing of black-market prices for health records—up to ten times more than credit card details—because compromised health records are used to perpetrate insurance fraud schemes, which take far longer to detect than credit card theft.[24]

According to research conducted in 2016, more than 90 percent of healthcare organizations have suffered from cyber attacks in the past two years, as hackers have sought medical records for their insurance fraud and identity theft schemes.[25] Given the rising cost of healthcare in the U.S., medical records are an increasingly attractive target: Using someone else's insurance information, thieves can ring up massive medical bills, leaving unsuspecting victims holding the bag.[26] Medical identity theft can be particularly harmful to consumers because it is very costly to resolve and can lead to higher premiums or loss of coverage. Each year, medical identity theft affects over 2 million consumers, costing the average victim more than $13,000 in the process.[27]

Encryption plays an important role in keeping stored health data secure in the event of such breaches. Notably, the Health Insurance Portability and Accountability Act (HIPAA), the main federal law governing electronic medical records, provides strong incentives for medical professionals to maintain health information in a secure manner that renders it "unusable, unreadable, or indecipherable" to unauthorized persons—a condition met by valid encryption processes.[28]

Cryptography also empowers consumers to play a role in advances in medical research that will

---

[22] H.R. 1 (2009), Sec. 4101(a)(o)(1)(D)(iii), *available at* https://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.

[23] Steve Lohr, *How to Make Electronic Medical Records a Reality*, N.Y. TIMES (Feb. 28, 2009), http://www.nytimes.com/2009/03/01/business/01unbox.html.

[24] *By the Numbers: Fraud Statistics,* COAL. AGAINST INS. FRAUD, http://www.insurancefraud.org/statistics.htm#13.

[25] Herb Weisbaum, *Cyber Attacks and Negligence Lead to Rise in Medical Data Breaches*, NBC NEWS (May 17, 2016), https://www.nbcnews.com/tech/tech-news/cyber-attacks-negligence-lead-rise-medical-data-breaches-n575471.

[26] *Medical Identity Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

[27] *Fifth Annual Study on Medical Identity Theft*, PONEMON INST. (Feb. 2015), http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

[28] *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERV. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

improve personalized medicine options and patient outcomes. For example, new cryptographic techniques are being developed that would let health app users, hospitals, and health organizations share patient data while preserving patient privacy, paving the way for major strides on important new medical research.[29]

Medical devices and virtual healthcare visits

The correct operation of connected medical devices can stand between life and death. Increasingly, the medical community and patients rely on such devices to monitor health conditions, deliver medications, and provide important safety notifications to doctors and their patients. And use of these devices could hold particular promise for consumers in underserved communities, who may not have sufficient access to traditional forms of healthcare.[30]

Tools for disease management and diagnostics, like drug infusion pumps, pacemakers, defibrillators, and health trackers, are all vulnerable to remote manipulation. In one case, a major device vendor successfully encrypted messages sent to a drug pump (meaning proper dosage information could not be manipulated in transit) but failed to instruct devices to check whether updates to information about dosage limits were sent from a trusted source.[31] This oversight meant that a malicious attacker could have tricked the pumps into releasing a dangerous dose of medication. More recently, an insulin pump was shown to be at risk of remote manipulation stemming from a failure to encrypt communication between the blood sugar monitor and the pump itself.[32]

To date, these risks have remained largely hypothetical, and there have been no widespread reports of tampering with medical devices. However, because security researchers have demonstrated the vulnerability of these devices, and because of the enormous potential for harm such vulnerabilities pose to consumers, medical devices should include the strongest possible digital safeguards. The Food and Drug Administration (FDA) has urged medical device makers to build in cryptographic authentication to make sure that software updates come from trusted sources.[33] Further, the Federal Trade Commission (FTC) and Department of Health and Human Services (HHS) have provided guidance reminding medical app developers that they may be required by the HIPAA Security Rule or the FTC Act to protect the confidentiality, integrity, and

---

[29] Ray Potter, *How Unvalidated Encryption Threatens Patient Data Security*, HEALTH IT SEC. (July 1, 2016), https://healthitsecurity.com/news/how-unvalidated-encryption-threatens-patient-data-security.

[30] *See Telehealth Use in Rural Healthcare*, RURAL HEALTH INFO. HUB (Aug. 2, 2017), https://www.ruralhealthinfo.org/topics/telehealth.

[31] Kim Zetter, *Hacker Can Send Fatal Dose to Hospital Drug Pumps*, WIRED (June 8, 2015), https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps.

[32] Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, REUTERS (Oct. 4, 2016), https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L.

[33] *Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*, U.S. FOOD & DRUG ADMIN. (Jan. 14, 2005), https://www.fda.gov/MedicalDevices/ucm077812.htm.

security of electronic medical records.[34] Moreover, networked medical devices in hospitals (most of which run on outdated operating systems[35]) provide attackers access to and the ability to manipulate data stored on the hospitals' networks, which are attractive and proven targets for hackers—highlighting the critical need for regular, secure software updates.

On top of monitoring patients with connected medical devices, many healthcare providers also offer virtual doctor visits, allowing patients and doctors to confer about physical and mental health issues via video chat and instant messenger systems. Successful implementation of telehealth programs could improve access to healthcare for inner city[36] and rural communities[37] that suffer from overcrowded health facilities and doctor shortages, as well as for older patients who have limited mobility.[38] And video-chat interventions show promising results in managing chronic diseases like diabetes—which disproportionately impacts minority patients, including those who may not be able to afford or have access to healthier food options or quality healthcare.[39]

But to use these services, patients must trust that interactions with their doctors are private—reassurance that end-to-end encryption can provide. And like other medical technology, telemedicine and many mobile health applications must comply with HIPAA, which as noted above provides strong incentives to providers to encrypt their data.[40]

Safeguarding consumers' financial well-being

Consumers have a powerful interest in the security of their money. Impenetrable safes historically served as protection for physical currencies, but as financial transactions have moved

---

[34] *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[35] Lily Hay Newman, *Medical Devices Are the Next Security Nightmare*, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare.

[36] *See* Kenneth M. McConnochie et al., *Telemedicine Reduces Absence Resulting From Illness in Urban Child Care: Evaluation of an Innovation*, PEDIATRICS (May 2005) *available at* http://pediatrics.aappublications.org/content/115/5/1273.short; Dorota T. Kopycka-Kedzierawski & Ronald J. Billings, *Teledentistry in Inner-City Child-Care Centres*, J. OF TELEMEDICINE & TELECARE (2006) *available at* http://journals.sagepub.com/doi/pdf/10.1258/135763306777488744; Kenneth M. McConnochie et al., *Telemedicine in Urban and Suburban Childcare and Elementary Schools Lightens Family Burdens*, TELEMEDICINE & E-HEALTH 16(5), 533-542 (June 2010) *available at* https://doi.org/10.1089/tmj.2009.0138.

[37] JT Ripton & C. Stefan Winkler, *How Telemedicine Is Transforming Treatment in Rural Communities*, BECKER'S HOSP. REVIEW (Apr. 8, 2016), https://www.beckershospitalreview.com/healthcare-information-technology/how-telemedicine-is-transforming-treatment-in-rural-communities.html.

[38] Melinda Beck, *How Telemedicine Is Transforming Health Care,* WALL ST. J. (June 26, 2016), https://www.wsj.com/articles/how-telemedicine-is-transforming-health-care-1466993402; Vera Gruessner, *Telehealth Services Improve Geriatric Care in Rural Settings*, MHEALTH INTELLIGENCE (Oct. 2, 2015), https://mhealthintelligence.com/news/telehealth-services-improve-geriatric-care-in-rural-settings.

[39] Ernest L. Carter et al., *A Patient-Centric, Provider-Assisted Diabetes Telehealth Self-management Intervention for Urban Minorities*, PERSPECTIVES IN HEALTH INFO. MGMT. (2011), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3035826.

[40] *See Guidance*, *supra* note 27.

into the virtual realm, cryptography now serves the same purpose for the modern consumer.

Digital financial transactions

Consumers purchased nearly $400 billion of goods and services online in 2016,[41] and 61 percent of U.S. internet users accessed their money through online and mobile banking portals.[42] HTTPS protects both these and other online financial transactions, such as the electronic filing of federal taxes and the submission of the Free Application for Federal Student Aid, which both require users to share sensitive details, from Social Security numbers to medical expenses.[43] Because of encryption, consumers can more confidently provide sensitive financial information to merchants through a website or app, a convenience that most Americans have come to expect as part of their daily lives.

Cryptography is also helping make financial transactions at physical stores and restaurants more secure. Chip-and-pin credit cards,[44] as well as most mobile payment systems like Apple Pay[45] and Android Pay,[46] use cryptography to authenticate transactions, and encryption enables private communication between banks and merchants, protects card details, secures the digital vaults that issue the single-use "tokens" to original card accounts, and safeguards the passcodes and fingerprint data used to validate mobile payments.[47]

These protections are making a dent in fraud: Roughly 9 out of 10 Americans now use chip cards,[48] and Visa and Mastercard reported 47 percent and 54 percent decreases, respectively, in fraud for secure chip card transactions.[49]

---

[41] *US E-Commerce Sales Grow 15.6% in 2016*, DIGITAL COMMERCE 360 (Feb. 17, 2017), https://www.digitalcommerce360.com/2017/02/17/us-e-commerce-sales-grow-156-2016.

[42] Susannah Fox, *51% of U.S. Adults Bank Online*, PEW RESEARCH CTR. (Aug. 7, 2013), http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online.

[43] Proper implementation of HTTPS and other digital security measures also protects students as they pursue other aspects of the financial aid application process. The U.S. Department of Education handles millions of applications for grants and loans, a process that is particularly critical for low-income families. When these online tools malfunction or are taken offline, the financial aid application process becomes longer and more difficult, and innocent mistakes can lead students to receive less aid than they are eligible for, or to get flagged for extra vetting, which delays access to much-needed funds. Molly Hensley-Clancy, *The FAFSA Just Became a Bigger Headache for Students*, CNBC (Apr. 5, 2017), https://www.cnbc.com/2017/04/05/the-fafsa-just-became-a-bigger-headache-for-students.html?view=story&%24DEVICE%24=native-android-mobile.

[44] *Credit Card Buying Guide*, CONSUMER REPORTS (Mar. 2017), https://www.ConsumerReports.org/cro/credit-cards/buying-guide.

[45] Yoni Heisler, *Apple Pay: An In-Depth Look at What's Behind the Secure Payment System*, ENGADGET (Oct. 2, 2014), https://www.engadget.com/2014/10/02/apple-pay-an-in-depth-look-at-whats-behind-the-secure-payment.

[46] *How Payments Work*, Android Pay, https://support.google.com/androidpay/merchant/answer/6345242?hl=en.

[47] Dan Schutzer, *Tokenization in Financial Services*, FIN. SERV. ROUNDTABLE (Mar. 2015), http://www.fsroundtable.org/cto-corner-tokenization-financial-services.

[48] *US Payments Forum Winter Market Snapshot*, EMV CONNECTION (Jan. 30, 2017), http://www.emv-connection.com/us-payments-forum-winter-2017-market-snapshot.

[49] Kevin Woodward, *A Year On, EMV Migration Achievements Beset With Ongoing Acceptance Challenges*, DIGITAL TRANSACTIONS (Sept. 29, 2016), https://www.digitaltransactions.net/a-year-on-emv-migration-

Identity theft and fraud

Identity theft can be devastating to consumers. It can drain their bank accounts; exhaust their health insurance benefits; depress their credit scores, which can hurt their ability to access a range of financial products; and even create criminal records in consumers' names. Even victims who successfully clean up their records and avoid major financial losses can suffer significant emotional distress, reputational damage, and loss of time and resources. Last year, $16 billion was stolen from 15.4 million Americans through identity theft; in the past six years, identity thieves have stolen over $107 billion from U.S. consumers.[50] One survey found that security breaches were more common in households using greater numbers of connected devices.[51]

Identity theft can hit low-income consumers especially hard: On top of losing money, victims risk their utilities being cut off, losing access to social benefits and affordable housing,[52] improper garnishment of wages[53] or child support,[54] and even wrongful arrest.[55] More than half of criminal identity theft victims reported needing to miss time from work[56]—but low-income victims may not be able to take time off from work or afford legal counsel to resolve the situation. The resulting tarnished credit and criminal records can make it difficult to pass background checks required to get jobs in the future.[57]

---

achievements-beset-with-ongoing-acceptance-challenges.

[50] Javelin Strategy & Research, *2017 Identity Fraud: Securing the Connected Life* (Feb. 1, 2017), https://www.javelinstrategy.com/coverage-area/2017-identity-fraud.

[51] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[52] "... for low-income individuals and families, the ... other effects experienced by identity theft victims across the income spectrum are often compounded by severe and immediate consequences to crucial needs-based benefits, subsidized housing, employment, utility service, and medical care. To cite one example, SBLS often sees clients whose need-based [Supplemental Security Income] benefits are threatened due to fraudulent earnings appearing on their records. ... Barriers such as limited English proficiency and limited phone and computer access increase the need for advocacy assistance in addressing identity theft affecting low-income clients." Sarah Dranoff, *Identity Theft: A Low-Income Issue*, 17 A.B.A. J. 2 (2014), *available at* https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue.html.

[53] *Id*.

[54] Adam Levin, *The Invisible Victims of Identity Theft: Our Kids*, ABC NEWS (Nov. 14, 2015), http://abcnews.go.com/Technology/invisible-victims-identity-theft-kids/story?id=35184348.

[55] Steve Weisman, *When Identity Thieves Commit Crimes in Your Name*, USA TODAY (May 21, 2016), https://www.usatoday.com/story/money/columnist/2016/05/21/when-identity-thieves-commit-crimes-your-name/84383670.

[56] *Identity Theft: The Aftermath 2016*, IDENTITY THEFT RES. CTR. (2016), http://www.idtheftcenter.org/aftermath-2016.html; Jesse Campbell, *Identity Theft Affects Much More Than Just Your Money*, MONEY MGMT. INT'L (Oct. 19, 2016), http://www.moneymanagement.org/Community/Blogs/Blogging-for-Change/2016/October/Identity-theft-affects-much-more-than-just-your-money.aspx.

[57] Marc Weber Tobias, *Your Credit Report and Identity Theft: What You May Not Know*, FORBES (Mar. 19, 2015), https://www.forbes.com/sites/marcwebertobias/2015/03/19/your-credit-report-and-identity-theft-what-you-may-not-know/#19a12a6063c6.

Cryptography is not a panacea for identity theft, but it can provide a last line of defense when important computer systems are compromised. Encryption of sensitive databases makes it more difficult for hackers to extract usable information during system breaches: When Adobe suffered a breach in 2013, at least 38 million customer records were compromised, but the damage was reduced because credit and debit card details included in the breach had been encrypted.[58] The situation was very different when the U.S. Office of Personnel Management system was breached in 2015. That time around, millions of sensitive government personnel records, including everything from Social Security numbers to the highly personal information compiled during security clearances, were compromised because the files weren't encrypted—in some cases because the agency's computer hardware was antiquated.[59]

As of early 2016, slightly more than half of financial services organizations worldwide are using encryption technology to safeguard their data, up from 43 percent in 2013.[60] While there is still room for improvement, encryption is clearly a critical ingredient in securing personal and financial information.

Facilitating safe software updates

Cryptography does more than protect the data flowing through websites and mobile apps. In fact, its importance is dramatically expanding as more consumer goods enter the marketplace embedded with software that must be kept up-to-date and secure.

Cryptography is essential to the delivery of these updates, as it allows a device to know *who* is installing *what*. Manufacturers use digital signatures to ensure that only genuine updates are delivered, guarding against code that might be sent from malicious actors, such as criminals looking to remotely turn on microphones, steal data, or attack other nearby devices.[61] This is not a theoretical danger: Users of Adobe Flash, Android, and multiple web browsers have been targeted in the past with invitations to download and install fake software updates.[62]

The problem could become more acute as consumers adopt a coming tidal wave of new software-driven devices. Mobile phones have become omnipresent and virtually omniscient personal assistants, with minority and vulnerable consumers being especially likely to be

[58] Alex Konrad, *After Security Breach Exposes 2.9 Million Adobe Users, How Safe Is Encrypted Card Data?*, FORBES (Oct. 9, 2013), https://www.forbes.com/sites/alexkonrad/2013/10/09/how-safe-is-encrypted-card-data-adobe/#428663306798.
[59] Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government.
[60] *Encryption Application Trends Study*, PONEMON INST. (June 2016), http://go.thalesesecurity.com/rs/480-LWA-970/images/AR-Encryption-Application-Trends-Study-2016.pdf.
[61] Yann Loisel & Stephane di Vito, *Securing the IoT*, EMBEDDED (Jan. 11, 2015), https://www.embedded.com/design/safety-and-security/4438298/Securing-the-IoT-Part-1-Public-key-cryptography.
[62] Danny Palmer, *Beware This Android Banking Malware Posing as a Software Update*, ZDNET (June 23, 2017), http://www.zdnet.com/article/beware-this-android-banking-malware-posing-as-a-software-update.

dependent on smartphones for their access to the internet.[63] Homes are becoming "smarter" as embedded, largely invisible computer chips control televisions, refrigerators, thermostats, home cameras, and light switches. Even cars—once the quintessential mechanical product—now depend heavily on digital technologies.[64]

To use all of these digital products and services, consumers must blindly trust hundreds of millions of lines of computer code as they navigate their day-to-day lives. And just as programmers spend their days creating and improving their code, hackers work hard at finding vulnerabilities that can enable them to turn baby monitors into spy devices,[65] infiltrate mobile phones and laptops,[66] and potentially even control a car's brakes and steering.[67] Many of these vulnerabilities carry the risk of being exploited in an environment where the stakes are high: Hackers have remotely hijacked connected Jeeps,[68] redirected yachts by "spoofing" GPS coordinates,[69] and locked home thermostats at 99 degrees Fahrenheit.[70] If these connected products used encryption, it would be much harder for hackers to exploit these vulnerabilities and place consumers at risk.

In this densely interconnected digital environment, a flaw in one device can lead to attacks on others. Already, new forms of malware, software that is intended to damage or disable computers and computer systems, can co-opt networked consumer devices such as webcams and teakettles to form "botnets" that perpetrate distributed denial-of-service (DDoS) attacks meant to disrupt access to websites and servers—usually without the device owner's knowledge.[71] And as more

---

[63] Monica Anderson & John B. Horrigan, *Smartphones Help Those Without Broadband Get Online, But Don't Necessarily Bridge the Digital Divide*, PEW RESEARCH CTR. (Oct. 3, 2016), http://www.pewresearch.org/fact-tank/2016/10/03/smartphones-help-those-without-broadband-get-online-but-dont-necessarily-bridge-the-digital-divide; Alessandra Ram, *For Homeless LGBTQ Teens, a Phone Can Be a Lifesaver*, WIRED (July 6, 2015), https://www.wired.com/2015/07/homeless-lgbtq-teens-phone-can-lifesaver.

[64] Richard Viereckl et al., *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles*, STRATEGY& (Sept. 28, 2016), https://www.strategyand.pwc.com/reports/connected-car-2016-study.

[65] Anthony Cuthbertson, *How to Protect Baby Monitors From Hackers*, NEWSWEEK (Jan. 29, 2016), http://www.newsweek.com/how-protect-baby-monitors-hackers-421104.

[66] Kate Murphy, *Build Up Your Phone's Defenses Against Hackers*, N.Y. TIMES (Jan. 25, 2012), http://www.nytimes.com/2012/01/26/technology/personaltech/protecting-a-cellphone-against-hackers.html?mcubz=0.

[67] Jordan Golson, *Jeep Hackers at It Again, This Time Taking Control of Steering and Braking Systems*, THE VERGE (Aug. 2, 2016), https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek.

[68] Andy Greenberg, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, WIRED (Aug. 1, 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks.

[69] Eric Berger, *Texas Students Fake GPS Signals and Take Control of an $80 Million Yacht*, CHRON (July 29, 2013), http://blog.chron.com/sciguy/2013/07/texas-students-fake-gps-signals-and-take-control-of-an-80-million-yacht/?cmpid=hpfc.

[70] Darlene Storm, *Hackers Demonstrated First Ransomware for IoT Thermostats at DEF CON*, COMPUTERWORLD (Aug. 8, 2016), https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html.

[71] *See, e.g.*, the October 2016 botnet attack. Sam Thielman & Elle Hunt, *Cyber Attack: Hackers 'Weaponised' Everyday Devices With Malware*, THE GUARDIAN (Oct. 22, 2016), https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-

employees bring their own consumer devices to work—and more equipment is connected to the internet—businesses, government agencies, and critical infrastructure will have to account for a far greater attack surface for criminals to exploit.

Programmers and criminals are in a perpetual information-security arms race. Widely deployed software must be regularly updated or it will quickly become insecure. And consumers depend on manufacturers to deliver frequent software updates to "patch" vulnerabilities as they are identified. In the ideal case for consumers, whenever a bug is discovered it is quickly reported to the vendor, who then fixes the computer code and pushes out a software update to vulnerable devices—all before a malicious hacker can exploit it.

Additionally, products may require updates to safeguard consumers even when no hackers or malware are involved. With cars now relying heavily on software, manufacturers are increasingly beaming updates to their vehicles to install bug fixes or improvements to safety features such as automatic emergency braking.[72]

> "Automatic updates are an important way that software companies ensure their users are as protected as possible from attackers, without inconvenience, significant effort, or technical savvy on the part of the user (who is more likely to install security updates when there is little or nothing she needs to do)."
>
> *—iPhone Security and Applied Cryptography Experts (legal motion in Apple v. FBI)*[73]

To be most effective, these updates must be delivered quickly and conveniently—yet people often avoid manually installing critical software. In fact, a 2012 survey found that 42 percent of Americans neglected to install software updates when prompted, with a quarter of survey respondents unaware of the importance of these upgrades.[74] That is why automatic updates are so appealing: The user does not have to do anything to benefit from security and performance improvements. But whether consumers have a hands-on role in the process or not, cryptography plays an indispensable part in facilitating software updates that enable their many devices to function.

---

malware-to-mount-assault.

[72] Will Oremus, *How Tesla Fixed a Deadly Flaw in Its Autopilot*, SLATE (Sept. 12, 2016), http://www.slate.com/articles/technology/future_tense/2016/09/how_tesla_s_software_update_fixed_a_deadly_flaw_in_autopilot.html.

[73] iPhone Security and Applied Cryptography Experts in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, Brief of Amici Curiae, U.S. District Court Central District of California, March 22, 2016, https://docslide.us/documents/cis-technologists-apple-brief-final.html.

[74] Katherine Noyes, *Too Busy for That Software Update? Survey Says: Join the Club*, PCWORLD (July 23, 2012), https://www.pcworld.com/article/259689/too_busy_for_that_software_update_survey_says_join_the_club.html.

Ensuring physical safety

The distinction between physical and virtual space is blurring as consumers increasingly rely on digital devices—from GPS-enabled mobile phones to fitness trackers to connected vehicles—in their daily lives. These technologies have made maneuvering the world easier, but they also mean that vulnerabilities in the digital realm can affect the physical one.

Emergency communications

When a disaster strikes, the public needs trusted communication channels to receive vital safety information. Without credible emergency instructions, chaotic situations can spark panic and put people in harm's way. In 1971, for example, an erroneous message was broadcast on TV and radio about an imminent nuclear attack,[75] and in 2013 a hacker managed to broadcast an alert about zombie attacks in California, Michigan, and Montana, and New Mexico.[76] In early 2017, someone managed to activate more than 150 emergency outdoor warning sirens in Dallas, terrifying residents in the middle of the night.[77]

The Federal Emergency Management Agency (FEMA) uses cryptography to protect the federal Emergency Alert System and safeguard America's emergency channels.[78] Created during the Cold War, the system operates at a national level to deliver critical information about missing persons and imminent threats from severe weather, terrorists, and chemical spills via television, radio, and mobile device alerts. These alerts can also contain public safety instructions like evacuation orders or shelter in place commands. Wireless Emergency Alerts—messages sent to consumer mobile devices—let authorities target specific geographic areas by pushing brief notices to all devices that are connected to cell towers within the alert zone. These rapid warning systems can be critical to residents of rural communities who are frequently exposed to extreme weather events.

> "Wireless emergency alerts are a very powerful tool that can reach a really large amount of people, even millions. Imagine if you could reach one million people saying

[75] Jesus Diaz, *This Message From NORAD Announced Global Nuclear War—In 1971*, GIZMODO (July 5, 2012), http://gizmodo.com/5923528/this-message-from-norad-announced-world-nuclear-war-in-1971.
[76] Kim Zetter, *This Is Not a Test: Emergency Broadcast Systems Proved Hackable*, WIRED (July 8, 2013), https://www.wired.com/2013/07/eas-holes.
[77] Claire Ballor et al., *Hacking Blamed for Emergency Sirens Blaring Across Dallas Early Saturday*, DALLAS NEWS (Apr. 8, 2017), https://www.dallasnews.com/news/dallas/2017/04/08/emergency-sirens-blare-across-dallas-county-despite-clear-weather.
[78] "EAS messages are composed of a digitally encoded header, attention signal, audio announcement and digitally encoded end-of-message marker." *Emergency Alert System (EAS) Fact Sheet*, FED. EMERGENCY MGMT. AGENCY (Jan. 1, 2016), https://www.fema.gov/media-library-data/1465326763240-4152791226bbd49cf46aff8cd5f43bb1/Emergency_Alert_System_Fact_Sheet_2016.pdf.

there was a tsunami coming, 'please run to the hills.' People trust the emergency alert system. They don't think it could be someone with bad intentions making the alert."

—Cesar Cerrudo, *Chief Technology Officer of security firm IOActive*[79]

Cryptography is what prevents anyone other than official "Alert Originators" from broadcasting messages. Only messages that have been digitally signed with a legitimate key can pass through FEMA's system and be forwarded to cell phone users. If this key were compromised, it would be all too easy for more bad actors to send out false alerts.

Automated vehicles

People's eyes and ears are no longer the only sources of information that cause a car's brakes to activate or an airplane to adjust its course. Such action is increasingly guided, and even automatically triggered, by other data inputs. Dozens of sensors and other sources of telemetry data feed real-time calculations that determine how vehicles will behave in a physical environment.[80] This new technology could help people with otherwise limited mobility, such as injured veterans or the blind, regain independence, and promises to reduce car crashes attributable to driver error[81]—a leading cause of injury and death in America.[82]

A steady stream of reliable, authentic data stands between consumers and disaster: A car that suddenly engages its brakes because it senses an obstruction that is not actually there could cause an accident;[83] a plane that follows false GPS coordinates could fly perilously close to a mountain or another plane;[84] and if a hacker gained control of hundreds or thousands of vehicles[85] and

[79] Peter Moskowitz, *Our Cell Phone Alerts Will Be Hacked*, WIRED (Sept. 29, 2016), https://www.wired.com/2016/09/our-cell-phone-alerts-will-be-hacked/.
[80] Guilbert Gates et al., *The Race for Self-Driving Cars*, N.Y. TIMES (June 6, 2017), https://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html.
[81] Darrell M.West, *Moving Forward: Self-Driving Vehicles in China, Europe, Japan, Korea, and the United States*, BROOKINGS INST. (Sept. 20, 2016), https://www.brookings.edu/research/moving-forward-self-driving-vehicles-in-china-europe-japan-korea-and-the-united-states; Phil LeBeau, *The $7 Trillion Promise of Self-Driving Vehicles*, CNBC (June 1, 2017), https://www.cnbc.com/2017/06/01/the-7-trillion-promise-of-self-driving-vehicles.html.
[82] *Key Injury and Violence Data*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 19, 2016), https://www.cdc.gov/injury/wisqars/overview/key_data.html; *see* Hannah Nichols, *The Top 10 Leading Causes of Death in the United States*, MEDICALNEWSTODAY (Feb. 23, 2017), https://www.medicalnewstoday.com/articles/282929.php.
[83] *See* Bruce Schneier, *Confusing Self-Driving Cars by Altering Road Signs*, SCHNEIER ON SEC. (Aug. 11, 2017), https://www.schneier.com/blog/archives/2017/08/confusing_self-.html.
[84] Mark L. Psiaki & Todd E. Humphreys, *Protecting GPS From Spoofers Is Critical to the Future of Navigation*, IEEE SPECTRUM (July 29, 2016), https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation; *see* Scott Peterson & Payam Faramarzi, *Iran Hijacked US Drone, Says Iranian Engineer*, THE CHRISTIAN SCI. MONITOR (Dec. 15, 2011), https://www.csmonitor.com/World/Middle-

manipulated their ability to sense their surroundings, it could lead to countless injuries and widespread damage.[86] Experts have warned that "hacktivists could have lots of fun causing traffic jams [using faked GPS signals], while terrorist groups might want to direct a person's car to the point of ambush or kidnapping."[87]

These are not hypothetical concerns: In 2010, researchers found that many in-car wireless networks did not take steps to validate incoming data.[88] This oversight left vehicles vulnerable to false sensor messages that could, for example, make warning lights act erratically, potentially leading drivers to ignore real warnings. Another group of researchers managed to change the course of a large yacht by feeding false GPS information to the ship's navigation system, which trusted it was receiving valid data from actual satellites.[89]

And as recently as 2014, researchers found that communication between certain traffic control systems and traffic lights was not encrypted, meaning an attacker could directly change lights in 100,000 intersections across North America.[90] The National Highway Traffic Safety Administration's proposed rules governing vehicle-to-vehicle communications include a requirement that cryptographic authentication validate the authenticity and integrity of messages exchanged between vehicles and their surroundings.[91]

Cryptography protects consumers from irregular—and potentially dangerous—behavior triggered by invalid data by making sure that the sources of information are who they claim to be, and secure software updates ensure that the code behind devices that move around in the physical world is not compromised. As with corporate data breaches, the evidence shows that the world needs more encryption, not less.

East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer (An Iranian engineer helped enable the capture of a U.S. drone by spoofing the GPS signals the drone was relying on).

[85] *See* Simson Garfinkel, *Hackers Are the Real Obstacle for Self-Driving Vehicles*, MIT TECH. REVIEW (Aug. 22, 2017), https://www.technologyreview.com/s/608618/hackers-are-the-real-obstacle-for-self-driving-vehicles.

[86] *See* Cory Doctorow, *Car Wars*, DEAKIN UNIV. (Nov. 2016), http://this.deakin.edu.au/lifestyle/car-wars (In this work of speculative science fiction, the author describes a near-future where the roads are solely populated by driverless cars. The story details some of these possible outcomes.); *see also* Cory Doctorow, *The Problem With Self-Driving Cars: Who Controls the Code?*, THE GUARDIAN (Dec. 23, 2015), https://www.theguardian.com/technology/2015/dec/23/the-problem-with-self-driving-cars-who-controls-the-code.

[87] Olivia Solon, *Connected Cars Not Hacking It on All Security Fronts*, BUS. DAY (Aug. 11, 2015), https://www.pressreader.com/south-africa/business-day/20150811/282016146052517.

[88] Ishtiaq Rouf et al., *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*, USENIX (Aug. 2010), https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rouf.pdf.

[89] *UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea*, UT NEWS (July 29, 2013), https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.

[90] Hal Hodson, *Traffic Light Hackers Could Cause Jams Across the US*, NEW SCIENTIST (Aug. 6, 2014), https://www.newscientist.com/article/mg22329814-600-traffic-light-hackers-could-cause-jams-across-the-us.

[91] *Notice of Proposed Rulemaking*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Jan. 12, 2017), https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications.

Communicating with confidence

Connected devices and new online services let consumers communicate and share information in productive and exciting ways. These communications must be robustly protected to ensure that all consumers can speak confidently in the digital realm without fear of harassment, embarrassment, or invasive surveillance. Additionally, consumers need to be able to communicate without fear that their conversations will be mined for information that could be used to discriminate against them.

Electronic communications

Many consumers choose to use encrypted communications apps on their phones to keep their conversations safe from prying eyes. Though the Fourth Amendment places limitations on government surveillance, consumers may lose their legal protections when communicating through a third party, such as an email service or telecommunications provider.[92] Statutory legal protections around the use of electronic communications services have not been significantly updated since 1986—well before widespread reliance on these technologies for so many aspects of our daily lives.[93] As a result, U.S. law enforcement may be able to obtain personal communications without a court-ordered warrant—and other countries around the world have even fewer legal protections. Beyond government surveillance, individuals communicating with one another have a legitimate interest in safeguarding conversations from people looking to eavesdrop for pecuniary or merely personal reasons.

Encrypted smartphone apps—like Signal and WhatsApp—make it much easier for consumers to protect their communications. Some apps also help consumers more strongly encrypt their voice calls as well. While normal cell phone calls typically use encryption, the protocols used by mobile networks have known vulnerabilities, so more secure options are sometimes necessary. Apps that provide strong encryption give consumers more confidence that their calls are secure.

Smartphone security

Smartphones are among the most personal and essential consumer devices on the market today.[94]

---

[92] The Fourth Amendment prohibits "unreasonable" government searches; typically the courts have required a warrant approved by a judge before law enforcement can search a person's property. However, a line of cases have held that citizens may not have the same expectation of privacy when they communicate or store data through an online service or cloud storage provider. Under this "third party doctrine," government may be able to access personal data under a far less stringent standard, potentially without court supervision. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009), *available at* http://repository.law.umich.edu/mlr/vol107/iss4/1.

[93] Mike Orcutt, *Why Congress Can't Seem to Fix This 30-Year-Old Law Governing Your Electronic Data*, MIT TECH. REVIEW (Feb. 17, 2017), https://www.technologyreview.com/s/603636/why-congress-cant-seem-to-fix-this-30-year-old-law-governing-your-electronic-data.

[94] *See, e.g.*, Press Release, Deloitte:, Americans Look at Their Smartphones More Than 12 Billion Times Daily, Even as Usage Habits Mature and Device Growth Plateaus (Nov. 15, 2017), *available at*

With the reams of personal and financial data generated by and living on these devices, smartphones are frequent targets for hackers, fraudsters, and others seeking to do consumers harm.[95]

Technology companies that make mobile operating system software—particularly Apple (iOS), Google (Android), and Microsoft (Windows Phone)—dedicate significant resources to releasing frequent patches for software security vulnerabilities that are discovered.[96] Often, these companies will issue multiple security updates in a month. To minimize opportunities for intruders to seriously compromise a mobile device, these mobile platforms require updates to be cryptographically signed to validate that the update is authentic and that it has not been intercepted and tampered with by a third party. While updates are not yet fully automatic, these providers, particularly Apple, prominently notify users when updates are available and make these updates easy to install.[97]

Cryptography provides manufacturers with the means to automatically keep phones up to date, but there is still much work to be done. In 2012, a survey found that all four major carriers sold "orphaned" devices, meaning they did not receive a single security or feature update after they came on the market.[98] Google's Android software has faced unique challenges because until now different device manufacturers and mobile carriers have often slowed the delivery of updates or failed to deliver updates altogether.[99] Google is working on a solution to this issue that would allow it to push vital security updates to Android phones with much shorter delays.[100] Nevertheless, Google reported that even just last year, more than half of Android phones in use had not received a security update in over a year.[101]

When smartphones are properly secured and updated, consumers are able to communicate with

---

https://www.prnewswire.com/news-releases/deloitte-americans-look-at-their-smartphones-more-than-12-billion-times-daily-even-as-usage-habits-mature-and-device-growth-plateaus-300555703.html.

[95] Allen St. John, *How Smartphones Are Becoming Hacking Targets*, CONSUMER REPORTS (Dec. 23, 2016), https://www.ConsumerReports.org/hacking/how-smartphones-are-becoming-hacking-targets.

[96] *See* Ashley Carman, *Apple's Latest Security Patch Fixes a Bug That Lets Hackers Take Over Your Phone via Wi-Fi*, THE VERGE (July 19, 2017), https://www.theverge.com/2017/7/19/16000206/ios-10-update-security-release; Kate Conger, *Android Plans to Improve Security Update Speed This Year*, TECHCRUNCH (Mar. 22, 2017), https://techcrunch.com/2017/03/22/security-updates-are-still-slow-for-android-users; Abrar Al-Heeti, *Applied Microsoft's Security Updates? You're Safe From KRACK*, CNET (Oct. 16, 2017), https://www.cnet.com/news/if-you-applied-windows-security-updates-youre-safe-from-krack.

[97] *See, e.g.*, Elissa Harrington, *Hacking Discovery Prompts Apple to Issue Urgent Alert to Update Your iPhone, iPad*, ABC 7 (Aug. 26, 2016), http://abc7ny.com/business/apple-issues-urgent-alert-to-update-your-iphone-ipad/1486196.

[98] Casey Johnston, *The Checkered, Slow History of Android Handset Updates*, ARS TECHNICA (Dec. 21, 2012), https://arstechnica.com/gadgets/2012/12/the-checkered-slow-history-of-android-handset-updates.

[99] Simon Hill, *Android Is Losing Its Battle With Fragmentation, and You're Paying the Price*, DIGITAL TRENDS (Feb. 11, 2016), https://www.digitaltrends.com/mobile/what-is-android-fragmentation-and-can-google-ever-fix-it.

[100] Jacob Kastrenakes, *Android O Is Supposed to Make Android Updates Arrive Faster*, THE VERGE (May 12, 2017), https://www.theverge.com/2017/5/12/15632552/android-o-faster-updates-project-treble-google.

[101] Tom Spring, *Half of Android Devices Unpatched Last Year*, THREATPOST (Mar. 23, 2017), https://threatpost.com/half-of-android-devices-unpatched-last-year/124511.

confidence that their messages and transactions are shielded from prying eyes. This is especially important as more and more Americans rely on these devices as their primary means of communication and access to the internet.[102]

> "As our nation's consumers and businesses turn to mobile broadband ... the safety and security of their communications and other personal information is directly related to the security of the devices they use."
>
> —*Federal Communications Commission Letter to Carriers*, May 9, 2016[103]

Authentication

One of the most challenging aspects of keeping consumers secure in the digital age is authentication. Today, most consumers have to rely on passwords, juggling a "mind-boggling array of personal codes squirreled away in computer files, scribbled on Post-it notes, or simply lost in the ether."[104] Because keeping track of passwords is so inconvenient and difficult, many consumers use simple passwords or reuse the same password on multiple services.[105]

> "Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed."
>
> —National Institute of Standards and Technology, Special Publication 800-63B[106]

These shortcuts lead to vulnerability. Simple passwords can be hacked or guessed, and repeated

[102] Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology.
[103] Jon Wilkins, *Letter to Carriers*, FED. COMM. COMM'N (May 9, 2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-339256A2.pdf.
[104] Jacob Bernstein, *It's as Easy as 123!@S*, N.Y. TIMES (June 22, 2012), http://www.nytimes.com/2012/06/24/fashion/computer-passwords-grow-ever-more-complicated.html.
[105] *Majority of Americans Reuse Passwords and Millennials Are the Biggest Culprits*, GLOBE NEWSWIRE (July 19, 2017), https://globenewswire.com/news-release/2017/07/19/1054094/0/en/SecureAuth-Survey-Majority-of-Americans-Reuse-Passwords-and-Millennials-Are-the-Biggest-Culprits.html; *see also* Andrew Chaikivsky, *Everything You Need to Know About Password Managers*, CONSUMER REPORTS (Feb. 7, 2017), https://www.ConsumerReports.org/digital-security/everything-you-need-to-know-about-password-managers ("The vast majority of us either use weak passwords or resuse passwords on multiple accounts.").
[106] *Appendix A—Strength of Memorized Secrets*, NAT'L INST. OF STANDARDS & TECH., *available at* https://pages.nist.gov/800-63-3/sp800-63b/appA_memorized.html.

use of passwords means that when one website suffers from a breach, all of a consumer's accounts that share that password may be at risk.[107] Fortunately, cryptography is helping consumers adopt tools to more securely and conveniently authenticate themselves in the digital world.

Password managers allow consumers to easily create, store, and even automatically fill in strong and unique passwords for their different accounts. Obviously, it is essential that password managers keep consumers' account data secure. Thus, all reputable password managers make thorough use of encryption, ensuring that the consumer—and only the consumer—can access her account information and passwords on all of her devices.[108]

Conclusion

Cryptography is deeply woven into nearly every element of our society, from the critical infrastructure that maintains our democratic and commercial systems to the everyday activities and communications that animate our personal lives. Despite its fundamental importance to the integrity of our conversations, civil liberties, health, and countless other areas, the extraordinary scope and much of the machinery of cryptography remain largely invisible to the public. As a result, the continuing debate regarding civil liberties, national security, and "backdoors" has rarely focused on the value of encryption to everyday private and public life. The debate deserves a more fulsome understanding and appreciation of what's at stake for consumers every day. As a society, we will no doubt struggle with the trade-offs between these benefits and the needs of law enforcement. But we should not wait for another high profile FBI case or a massive data breach to wrestle with these important issues.

We hope this paper raises awareness about the many ways that encryption benefits consumers and the systems and infrastructure we rely upon, and the potential costs if encryption were to be compromised. In assessing the benefits and costs of encryption and backdoors, the public deserves a broader understanding of the critical role that cryptography plays in securing so many diverse aspects of our daily lives.

---

[107] John Patrick Pullen, *Why Your Passwords Are Easy to Hack*, TIME (Dec. 22, 2014), http://time.com/3643678/password-hack; Aimee Picchi, *Why Sites Are Bugging You to Reset Your Password*, CBS NEWS (June 17, 2016), https://www.cbsnews.com/news/why-sites-are-bugging-you-to-reset-your-password.

[108] *The Motherboard Guide to Not Getting Hacked*, MOTHERBOARD (Nov. 15, 2017), https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide.