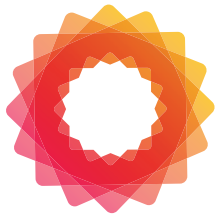
NUTS & BOLTS *of* ENCRYPTION

A primer for policymakers on encryption

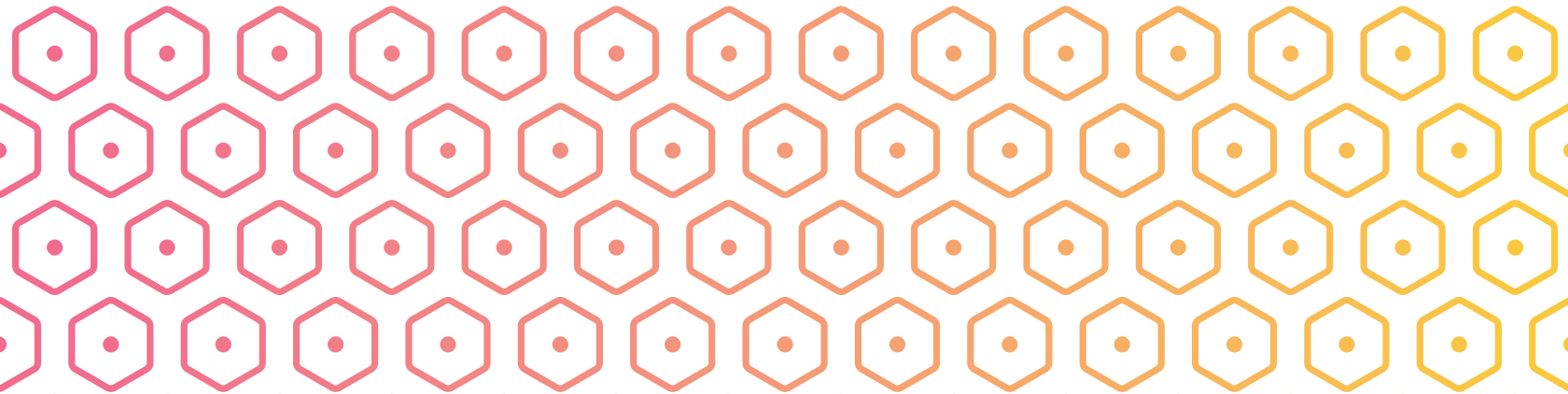
DECEMBER 2019

presented by:



Engine

CHARLES KOCH INSTITUTE



INTRODUCTION

Most of us use encryption every day, often without realizing it. From talking with loved ones, securing communications between Internet-connected devices, and storing and sharing sensitive health, banking, and business information, we all regularly rely on the security provided by encrypted products and services.

Despite how often we use encryption—and how prominent the encryption debate has become in policy circles—few understand how it actually works. Recently, the conversation about encryption has been framed as a conflict between a select number of high-profile technology companies and law enforcement, but this leaves out the perspective of Internet users and companies of all sizes—especially startups—that rely on encryption and will be impacted by any policy decisions that come out of this conversation.

In the fall of 2019, Engine and the Charles Koch Institute partnered on a three-panel series about "The Nuts and Bolts of Encryption" to educate policymakers and staff on how the technology behind encryption works, how it's used every day, and where the current debate over encryption stands today.

As a conclusion to this series, this report examines the concepts covered in the panels, beginning with an explanation of the mathematical principles behind encryption and the technical limits of those principles. At its core, encryption relies on the basic idea that it's very easy to combine two simple things into something complex, but it's very difficult to take a complex thing and separate it out into its simple components.

This report also examines several recent developments in the policy debate over encryption, including the debate over building backdoors to encrypted content for law enforcement, as well as reports about law enforcement's current capabilities and impediments to accessing data in criminal investigations, and growing concerns on how encryption may affect efforts to combat the spread of child exploitation material on the Internet.

Through the event series and this report, Engine and the Charles Koch Institute hope to add context and nuance to the debate around encryption, which shouldn't be reduced to a fight between large technology companies and law enforcement.

CONTENTS

WHAT IS ENCRYPTION?

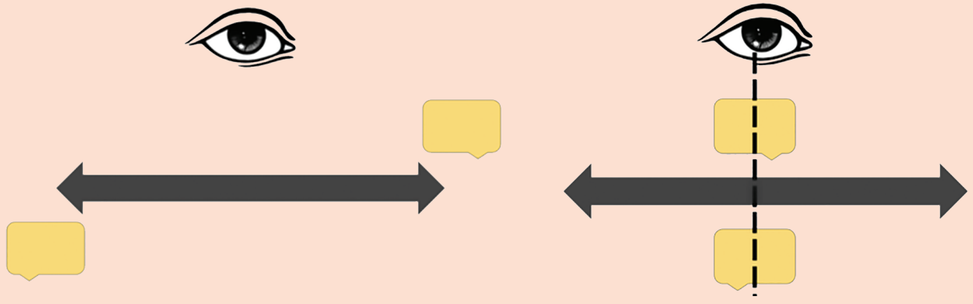
Encryption is a security tool that is used to protect data from access by unauthorized parties. Through encryption, data is "locked" and converted into an unreadable format that can only be "unlocked," or decrypted using a specific key, which is given to or held by authorized parties.

Cryptography, or the creation and solving of codes, in its general form dates back many centuries. Ancient Mesopotamians hid trade secret information using codes, and Julius Caesar used a cipher to encode military information. Since those early days, the art of hiding information using codes has advanced significantly. Today, with sophisticated computing technologies, algorithms are able to quickly generate unique ways to scramble data and hide it from prying eyes.

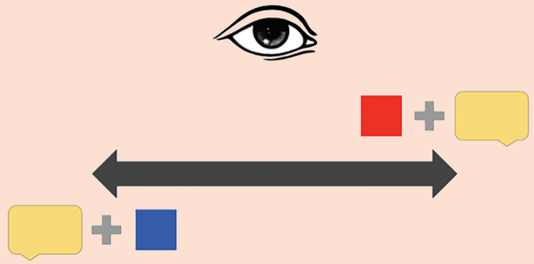
HOW DOES IT WORK?

Encryption relies on the basic idea that it's very easy to combine two simple things into something complex, but it's very difficult to take a complex thing and separate it out into its simple components.

The most common method for encrypting data relies on combining large numbers, but the concept can be demonstrated—at its most basic level—by combining primary colors.

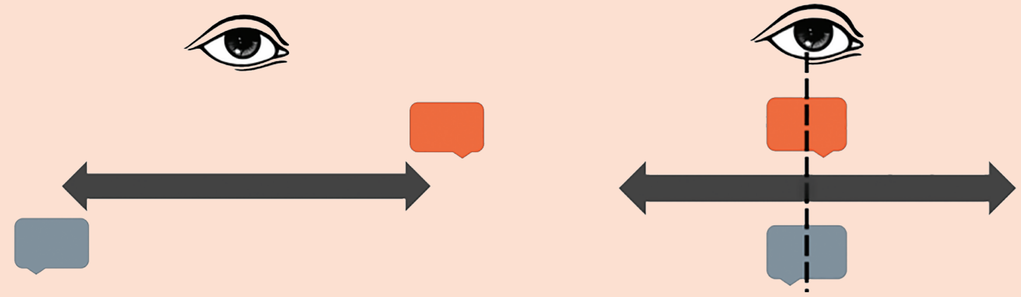


In the example above, two users are communicating over a network and through an encrypted messaging app. Each user is given two colors: either yellow and red or yellow and blue. The color yellow represents messages that are transmitted across the network in plaintext. If two parties exchange messages in their current form, a third party could easily intercept and read them.

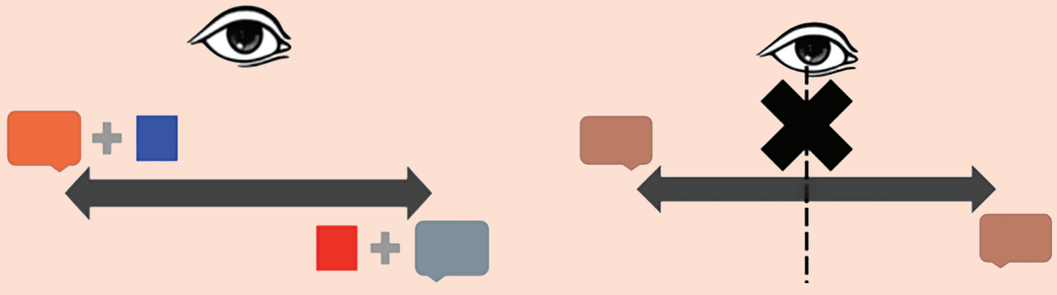


Each user can mix in a small amount of their secondary color—either red or blue—to "encrypt" the message they want to travel over the network. The resulting unique color represents a "private key" which belongs to an individual and is used to scramble data and protect it from unauthorized viewers. In many common encryption applications today, users don't even realize they're using a private key to protect their data, because their key lives inside the encrypted device or service they're using.

Now the colors have been mixed—or the data has been encrypted—the messages can be sent across the network without a third party understanding what they contain.



Once both parties receive the encrypted message, they have to be decrypted. To do this, each user will match the color they received with the color representing their private key. Both messages will now be "decrypted," or the same color. Since the color never passed over the network, no unauthorized third party could see the final product.



GLOSSARY

Encryption at-rest
When data is encrypted "at-rest," this means it is being stored securely in one place, most commonly on one device.

Encryption in transit
When data is encrypted "in transit," this means it is protected as it's being transmitted from one party to another, usually across a network.

Encryption in the cloud
When data is encrypted at rest when being held by a cloud service provider.

Asymmetric encryption
If encryption is asymmetric, two different keys are used to encrypt and decrypt data. This is commonly used in online services.

Symmetric encryption
If encryption is symmetric, the key used to encrypt data is also used to decrypt data. All parties involved in exchanging the data agree upon the key before the data is encrypted.

Backdoor
An intentionally constructed vulnerability in an encrypted product or service that is usually designed for law enforcement to access encrypted data.

Private key
The closely-held key that allows a recipient to decrypt data that has been encrypted using the paired public key. The key must be kept secret to preserve the security of a system of asymmetric encryption.

Public key
Asymmetric encryption (see above) uses two types of keys—one public and one private—and you need a pair comprising of each to successfully encrypt and decrypt data. A person's public key can be shared widely to allow anyone to encrypt their communications to that person.

Encryption
The process by which data is scrambled or converted to a format unreadable by those not authorized to access the data.

End-to-end encryption (E2EE)
Communications that are encrypted end-to-end can only be viewed by the sender and receiver. No other party that may see the data as it travels between the sender and recipient—including Internet service providers, hackers, and application providers—can decrypt the data.

Ephemeral key
A key that is regenerated in each key establishment process and is designed to be used once or in a single session. This differs from static keys which are designed to be used repeatedly over time.

NCMEC
National Center for Missing and Exploited Children, a non-profit established by Congress that works with private companies and law enforcement to combat child abduction, abuse, and exploitation. NCMEC acts as a clearinghouse and reporting center for child exploitation material.

Man-in-the-middle attack
An attack where a third party intercepts a communication between a sender and recipient. The third party might then read, or even alter, the communication before it reaches the recipient.

Plaintext
Data that is unprotected and has not yet been inputted into an encryption algorithm, or that is the output of decryption. Sometimes this term is used interchangeably with "cleartext" but, technically speaking, cleartext refers to unprotected data that is not intended for encryption.

RESPONSIBLE TO WHOM? AN ENCRYPTION SIMULATION

INSTRUCTIONS:

THE STORY:

You are a member of the security team at StartNet, a startup that provides network security for hundreds of platforms, websites, and applications.

The FBI has approached you because they have reason to believe that a terrorist organization is communicating using PlotChat, a chat client that runs on one of StartNet's encrypted networks. The FBI thinks terrorists are planning a potential attack using PlotChat.

You've identified specific U.S. users and traffic patterns on your network associated with PlotChat and have provided options for the FBI to get information about those users, including providing metadata about PlotChat users and communications.

Instead, the FBI wants you to build a "backdoor" into your network so that agents can intercept PlotChat messages. The agency has threatened to take you to court and a government source has leaked to the press that the FBI and StartNet are talking about building a backdoor.

THE OBJECTIVE:

In two weeks you must decide whether to cooperate with the FBI and build a backdoor into your network encryption. Before then, you'll speak with five different stakeholders and announce after each one whether or not StartNet will cooperate with the FBI. That answer will affect the number of points you have in the following three categories: User Trust, Government Cooperation, and Revenue.

Start with 30 points in each category. Every round you will make a decision which will add or subtract points in each category.

	USER TRUST	GOVERNMENT COOPERATION	REVENUE
APPROACHED BY FBI:	30	30	30
Round 1: Other Users			
Round 2: Malicious Actors			
Round 3: International Competition			
Round 4: Business Costs			
Round 5: Foreign Governments			
YOUR TOTALS:			

START

ROUND 1: OTHER USERS
You're approached by SafeHouse, a non-profit that works with domestic abuse victims. They use a chat app that runs over your encrypted networks to provide help to victims. They warn you that domestic abusers have already attempted to hack the chat app and harass victims.

If StartNet builds a backdoor, it will significantly weaken the security of the app and risk the safety of domestic abuse victims. SafeHouse will have to stop using any app run over StartNet networks, and it will publicly encourage other victims' groups to do the same.

ANNOUNCE PLANS TO AGREE TO BUILD BACKDOOR

-10 user trust
+5 government cooperation

ANNOUNCE PLANS TO REFUSE TO BUILD BACKDOOR

+5 user trust
- 6 government cooperation

ROUND 2: MALICIOUS ACTORS
A major data breach is revealed at competing network security company, NotLock. Press reports revealed the company built a backdoor into its network encryption tools in 2014 at the behest of the DEA, which was investigating a drug cartel using NotLock's services.

A group of malicious hackers in Argentina found and exploited that vulnerability. They've intercepted and published data from NotLock's secure networks, including emails between executives at a Fortune 500 company relating to a hiring scandal.

Your clients are concerned about the risk to their businesses if StartNet creates a similar backdoor.

ANNOUNCE PLANS TO AGREE TO BUILD BACKDOOR

-10 user trust
+5 government cooperation

ANNOUNCE PLANS TO REFUSE TO BUILD BACKDOOR

+5 user trust
- 6 government cooperation

ROUND 3: INTERNATIONAL COMPETITION
Canadian network security company MapleNet launches an aggressive ad campaign touting their break-proof encryption tools to Fortune 500 companies in the U.S. MapleNet is telling your clients that its encryption is better than StartNet's because they are outside of the FBI's reach and can't be compelled to build in a backdoor.

Your Fortune 500 clients are threatening to take their business to MapleNet.

ANNOUNCE PLANS TO AGREE TO BUILD BACKDOOR

-10 revenue
+5 government cooperation

ANNOUNCE PLANS TO REFUSE TO BUILD BACKDOOR

+2 revenue
- 6 government cooperation

ROUND 4: BUSINESS COSTS
To comply with the FBI's request and maintain reasonable network security practices, StartNet will have to either reassign several engineers or hire new engineers to build the vulnerability and then protect it from attacks by malicious actors.

Reassigning engineers would require pausing the development of new network security tools that StartNet was hoping to bring to the market later this year. Hiring new engineers will cost hundreds of thousands of dollars.

ANNOUNCE PLANS TO AGREE TO BUILD BACKDOOR

-10 revenue
+5 government cooperation

ANNOUNCE PLANS TO REFUSE TO BUILD BACKDOOR

+2 revenue
- 6 government cooperation

ROUND 5: FOREIGN GOVERNMENTS
A global digital rights and civil liberties group alerts you to an effort by Australian policymakers to require domestic technology companies to build intentional vulnerabilities into their products. The group warns StartNet that if it builds a backdoor for the FBI, Australian law enforcement will increase pressure on other companies to build similar backdoors into their products.

Your international compliance team warns that the costs of complying with backdoor requests from several countries will require several more engineers and international lawyers.

ANNOUNCE PLANS TO AGREE TO BUILD BACKDOOR

-10 user trust
-10 revenue
+5 government cooperation

TALLY SCORE ON PAGE 6

ANNOUNCE PLANS TO REFUSE TO BUILD BACKDOOR

+5 user trust
+2 revenue
- 6 government cooperation

DECISION DAY

User Trust
If you have fewer than 20 points, StartNet will face public backlash and lose many of its users.

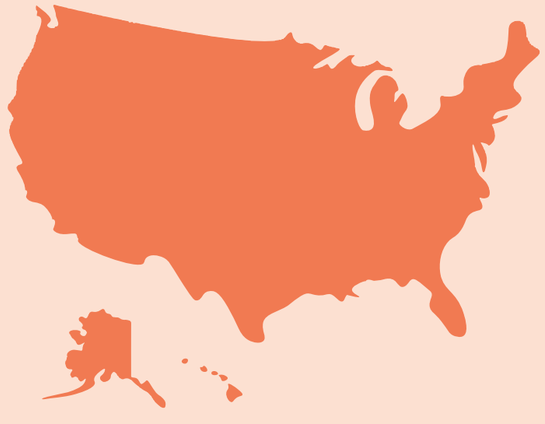
Revenue
If you have fewer than 15 points, StartNet will have to downsize its operations, laying off dozens of engineers.

Government Cooperation
If you have fewer than 24 points, the government will sue to compel StartNet to build in the backdoor, and the industry will face threats of legislation.

GLOBAL UPDATES

The last year has seen several developments in the policy debate over strong encryption in the United States and around the world. Like all Internet policy issues, the steps taken by foreign governments that either promote or hinder the use of strong encryption will impact global technology companies and their users around the world.

United States



Law enforcement officials in the United States have for years warned of the "going dark" problem: that as Internet users embrace encrypted products and services to protect their privacy and security, law enforcement is losing the ability to access digital evidence needed to combat crime.

In 2019, the Justice Department began focusing more intensely on the ways that secure encryption supposedly prevents law enforcement from combatting the creation and spread of child exploitation imagery on the Internet. Despite evidence that the major Internet platforms are increasingly finding and reporting child exploitation material in an effort to keep up with the ever-growing problem of child exploitation material online, U.S. officials in speeches and at events held by the Department of Justice have repeatedly criticized companies for allegedly erecting obstacles for law enforcement in pursuit of digital evidence.

The issue came to a head in 2019 when Facebook announced that it planned to use end-to-end encryption across its messaging platforms. The company faced backlash from domestic and international law enforcement officials who warned the move would impede law enforcement's investigations into serious and life threatening crimes, including those involving child exploitation. Experts in security, privacy, and technology communities defended Facebook and other companies offering encrypted products and services, warning that law enforcement's push to have companies build intentional vulnerabilities into their products will undoubtedly open a whole new set of safety and security concerns for Internet users that rely on encryption every day around the world.

The debate moved to the Hill towards the end of 2019 when the Senate Judiciary Committee held a December hearing about encryption and access to digital evidence. The majority of lawmakers at the hearing hammered technology companies that use encryption, accusing them of making it difficult for law enforcement to investigate and prosecute the most heinous crimes.

Australia

At the end of 2018, the Australian legislature passed a bill—introduced as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act—that allows law enforcement to force companies operating in Australia to turn over access to encrypted user data. The law was positioned as an anti-terrorism effort, but critics of the law say it will harm user security and safety. Since implementation, several news publications have spoken out about how the law has harmed journalists by chilling speech and impacting their ability to talk to sources securely.

United Kingdom

In late 2018, the United Kingdom's intelligence agency, Government Communications Headquarters (GCHQ), proposed a new way to let law enforcement access encrypted data that purportedly would avoid the security problems of forcing companies to build intentional vulnerabilities into their products. The so-called "ghost protocol" would have companies covertly insert law enforcement agents into encrypted communications. The individuals originally communicating would be unaware that law enforcement had been added as a silent observer. Supporters of the proposal argue that this would allow existing encryption security to remain intact while allowing law enforcement to collect digital evidence. But critics say the idea still raises concerns about user trust in encrypted products, as well as the security risks of undermining the way users of encrypted messaging services authenticate each other and any potential unintended vulnerabilities created to make this proposal possible.

Five Eyes

During the summer of 2019, the "Five Eyes"—an intelligence alliance made up of the U.S., the United Kingdom, Canada, Australia, and New Zealand—ramped up its opposition to strong encryption when it issued a statement calling on companies to comply with law enforcement's requests for encrypted data. After a July meeting in London, the group once again asked technology companies to not deliberately build their systems in ways that make it impossible for law enforcement to gain access to digital evidence. Mirroring U.S. officials' language, the Five Eyes statement warned that encryption can empower serious criminals to evade the law and put public safety at risk.

WHO ENCRYPTION PROTECTS

While the debate around encryption tends to center on criminals' use of secure technology to evade law enforcement, encryption provides a critical and even life-saving tool for many vulnerable communities.

DOMESTIC VIOLENCE SURVIVORS

Many domestic violence survivors rely on encrypted communications services to safely create a plan to escape from their abusers, or to avoid being spied on by their abuser. The heightened privacy and security that encryption provides allows domestic violence survivors to find resources, establish lifelines, and communicate about their location without having to worry about their abusers discovering their plans. If the companies providing those encrypted communications services were required to build in backdoors to facilitate law enforcement access, domestic violence survivors wouldn't be able to rely on those tools to protect them from their abusers. Even if the companies could ensure that outside abusers couldn't access the newly-created backdoor, there would be no way to ensure that individuals that commit domestic violence and work for tech companies or law enforcement wouldn't use the backdoor to target their victims.

LGBTQ+ COMMUNITY

For members of the lesbian, gay, bisexual, transgendered, and queer (LGBTQ+) community, encryption is often a necessary tool to ensure physical safety. For many in the United States, being outed as a member of the LGTBQ+ community can mean facing harassment and violence, losing your job, being kicked out of your home, and being cut off from your personal networks. Secure communications, including through encryption, can be what protects the ability of LGTBQ+ individuals to connect with each other and allies, safely explore otherwise hidden identities, and access critical resources.

The situation is even more dire in some countries around the world, where being a member of the LGBTQ+ community is considered a crime. In the U.S., the encryption debate is often framed as a request from law enforcement for help to go after criminals. But if tech companies comply with U.S. law enforcement's requests for intentional vulnerabilities in encrypted products and services, other governments—including in countries where being an LGTBQ+ individual is a crime—will ask for similar access or find ways to exploit those newly created vulnerabilities to go after anyone deemed a criminal, including members of the LGBTQ+ community.

HUMAN RIGHTS ACTIVISTS

Many human rights activists around the world use encrypted communications services to protect their identities and organizational efforts, including for activities like organizing protests. Creating a backdoor into those encrypted services would mean opening up activists to threats, including being identified and tracked and having adversaries intercept and potentially manipulate organizing communications. The result would undeniably be a chilling of speech, especially of speech on controversial and political topics.

While those in the United States have a right to protest and peaceably assemble, many other countries lack this basic right, and those countries' law enforcement could easily use an encryption backdoor to persecute activists and protestors. In 2019 alone, protesters in Hong Kong used encrypted messaging platforms to distribute information and organize demonstrations, and protesters in Moscow used the technically banned encrypted messaging service Telegram to communicate and gather aid for protesters who have been detained. In both instances, the activists using encryption tools to organize are facing police detainment and brutality. If a company offering an encrypted service builds in a backdoor at the behest of U.S. law enforcement, that backdoor could be used by foreign governments—with or even without the company's knowledge—to go after protesters in these kinds of situations.

JOURNALISTS

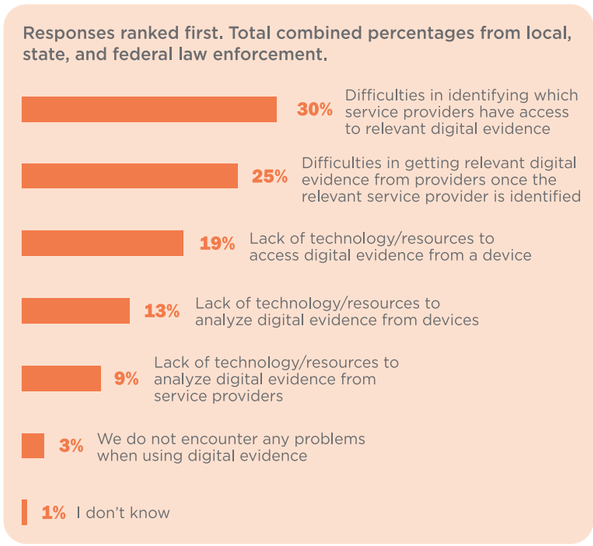
Many journalists rely on encryption to talk to sources and gather facts for their reporting. Especially for sources discussing some of the most sensitive and controversial topics—such as government whistleblowing, corporate malfeasance, or sexual harassment from high profile executives—confidentiality and security are paramount. If sources were to lose trust in the security of their communications with journalists, and therefore the ability of the journalist to keep their identity hidden, they would be even less willing to shed light on sensitive and controversial topics.

For reporters themselves, encryption provides a way to ensure the integrity of their reporting as well as their own personal safety. Ronan Farrow—whose reporting on film producer Harvey Weinstein's record of sexual assault allegations led to Weinstein's personal and professional downfall and contributed to a broader conversation about sexual harrassment—and his producer Rich McHugh reportedly used encrypted communications services to protect themselves and their sources from Weinstein's retaliation. "[M]y home in suburban New Jersey was broken into and the phone wires were tampered with," McHugh wrote in a Vanity Fair piece in 2019. "I began communicating through encrypted apps and burner phones, and told my wife and four daughters not to answer the door for any stranger."

WHAT CAN TECH DO?

Tech companies of all sizes want to cooperate with lawful law enforcement investigations, especially when it comes to dangerous and serious crimes such as child exploitation. Policymakers should find ways to increase this cooperation in ways that don't fundamentally undermine the privacy and security of their users—like building an intentional vulnerability into their encrypted products and services would.

Despite repeated claims from U.S. law enforcement officials, the evidence doesn't indicate that encryption is a major obstacle for law enforcement as they collect digital evidence. A 2018 report from the Center for Strategic and International Studies' Technology Policy Program—titled "Low-Hanging Fruit"—which included a survey of local, state, and federal law enforcement officials found that the biggest problems law enforcement faces in gathering digital evidence is "identifying which [companies] have access to relevant digital evidence" and "getting relevant digital evidence from [companies] once the relevant [company] is identified."



Though many tech companies already attempt to cooperate with law enforcement investigations, including by providing guidelines and trainings, the report noted a frustration that both technology companies and law enforcement feel when communicating, or miscommunicating, with each other. Law enforcement agents complained in the survey about long delays, incomplete information, and a lack of knowledge about the "magic words" that companies are looking for before they provide data to law enforcement. Companies complained about overly broad and boilerplate requests for data, as well as a lack of awareness of companies' responsibility to protect user data and privacy.

The report also highlights an inadequacy in overall training and resources for law enforcement to access and use digital evidence, including technical specialists, equipment, analytical tools, and legal expertise. The report offers recommendations to increase training and resources at the federal, state, and local levels and to increase cooperation between companies and law enforcement, including having companies commit to quick response times and provide information about why they reject law enforcement requests for data.

To learn more about this report, please visit CSIS:
https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge

CONCLUSION

Consumers are increasingly concerned about their data and skeptical of the companies that promise to keep and protect it. Encryption is one of the tools companies of all sizes can use to keep their users' data secure in a world of cyberstalking, corporate data breaches, and foreign government hacking.

Companies should be applauded for—not discouraged from—using tools like encryption to protect their users' data. This is especially true for the new and small companies that make up the U.S. startup ecosystem. Startups stand to lose the most in the debate over encryption. Unlike the large tech industry players, startups don't have long-standing reputations or relationships with users. When user trust in tech companies is shaken after something like a data breach, it's startups that users abandon first.

Law enforcement should have the tools it needs to combat serious crimes, such as child exploitation. Technology companies should do—and do—what they can to cooperate with law enforcement investigations that have appropriate judicial oversight, including complying with existing reporting requirements, educating law enforcement about platforms, and finding technological solutions to keep illegal material offline once it has been identified.

Forcing companies to build intentional vulnerabilities into their products and services will cause negative consequences for everyday Internet users that far outweigh potential benefits. Undermining the privacy and security for some will undermine the privacy and security of all, including human rights activists, reporters, domestic violence survivors, and members of persecuted communities. As one metaphor goes, criminals walk on the sidewalk, but you don't make the sidewalk crumble underneath everyone just to get at the bad guys.

The encryption debate clearly isn't going anywhere. As long as there are calls to have companies build intentional vulnerabilities into their encrypted products and services, there will be a need for a reasonable, nuanced, and fact-based conversation about how encryption works and how it's used everyday.

Engine was created in 2011 by a collection of startup CEOs, early-stage venture investors, and technology policy experts who believe that innovation and entrepreneurship are driven by small startups, competing in open, competitive markets where they can challenge dominant incumbents. We believe that entrepreneurship and innovation have stood at the core of what helps build great societies and economies, and such entrepreneurship and invention has historically been driven by small startups. Working with our ever-growing network of entrepreneurs, startups, venture capitalists, technologists, and technology policy experts across the United States, Engine ensures that the voice of the startup community is heard by policymakers at all levels of government. When startups speak, policymakers listen.

For more than five decades, Charles Koch's philanthropy has inspired bold new ideas to improve American lives. Inspired by a recognition that free people are capable of extraordinary things, the Charles Koch Institute supports educational programs and dialogue to advance these principles, challenge convention, and eliminate barriers that stifle creativity and progress. We offer educational programs, paid internships, and job placement assistance to students and professionals, and encourage civil discussion about important issues like free speech, foreign policy, and criminal justice reform. In all of our programs, we are dedicated to identifying new perspectives and ideas that help people accomplish great things for themselves and others.