Explaining Encryption

Center Forward Basics
June 2020

Overview

In an age where technology is a staple of business and commerce, personal livelihood, entertainment, and global interconnectivity, encryption is a crucial component to the protection of users' safety and privacy. Many consumers, often without realizing it, rely on encryption to protect their identity, personal communications, and live a normal life in a world of tech. Facing increased scrutiny from regulatory agencies, lawmakers, and law enforcement agencies, tech companies and others from the private sector are increasingly forced to answer a complex question: to what extent should they cooperate with law enforcement as encryption protections are challenged? Legal, financial, political, moral, and credibility considerations all need to be made in the process. This basic will explain what encryption is and consider some of the costs and benefits of encryption legislation.

What is Encryption and Why is it Important?

Encryption is the method of coding information to hide information's true meaning until it is decoded by its intended viewer. There are many different forms of encryption. End-to-End Encryption (E2EE) is used in systems such as ICloud, sms, and WhatsApp, among many other communication platforms. E2EE is a method of securing communication to prevent third-parties from accessing data while it's transferred from one end system or device to another. Another form is "Encryption At Rest", which is information stored or saved on a device or server. An example of this would be banking information stored in your phone. It's stored and sitting on your device or system but is not being sent anywhere. "Encryption In Transit" is coded information that is protected as it is transferred from one party to another. An example of this is when a purchase is made on a card and one's personal information is distributed to the necessary parties in a coded message to protect sensitive information. Data is stored either in a secured "Cloud" or on individual devices. Some companies allow specific devices to hold data and memory that is neither seen nor stored by the company, rather it allows the individual user to have personal encryption and privacy. While many enjoy having their information available from every one of their devices in case of device damage, personal and private encryption on singular devices can be appealing to consumers and tech companies, as it takes a liability component off of their shoulders.

Encryption as a security measure also protects some of the world's most vulnerable populations and is at the core of professions and organizations that preserve and protect institutions such as democracy, law, and a free press. This includes crime victims, oppressed minorities, immigrant and refugee groups, human rights organizations, financial advisors, medical professionals, and

Center Forward Basics

Center Forward brings together members of Congress, not-for profits, academic experts, trade associations, corporations and unions to find common ground. Our mission: to give centrist allies the information they need to craft common sense solutions, and provide those allies the support they need to turn those ideas into results.

In order to meet our challenges we need to put aside the partisan bickering that has gridlocked Washington and come together to find common sense solutions.

For more information, please visit www.center-forward.org

Key Facts

- **Encryption:** the method of creating secret code to hide information's real meaning.
- **End-To-End Encryption (E2EE):** secure communication that prevents third-parties from accessing data while being transferred.
- **Encryption At-Rest:** information that is sitting on a device/server that is saved/stored.
- **Encryption In Transit:** data that is being transmitted across a network.
- **"Backdoors":** purposeful vulnerabilities that companies leave so that outside actors can avoid using keys in order to decrypt information.

journalists. Even the government uses encryption on a daily basis. These groups rely on private servers to communicate without risk of judgment or publicizing personal or sensitive information. Encryption also allows parties to have private conversations virtually. During the COVID-19 pandemic, many patients have had virtual medical consultations with their doctors and doctors can now send test results and clinical notes over certain chat platforms.

Efforts to preserve private information involve encryption in various departments and levels of government. For example, the Internal Revenue Code Section 6103 stipulates that "the IRS must protect all personal and financial information furnished to the agency against unauthorized use, inspection or disclosure. Federal, State and local authorities who receive federal tax information" directly from the IRS or from secondary sources must have adequate security controls in place to protect the data received. Data encryption is crucial to everyday privacy of individuals including messaging, social media, shopping portals, banking information, cell phone companies, among many other systems.

In order to view encrypted information a person must either have access to a "key" which is the standard way of decrypting information or have a "backdoor" where they can decrypt information that is in transit or at rest. To decrypt information using "keys", one needs both a Public and Private Key. Public Keys are similar to addresses, in that in order to deliver information, the sender must know who they are sending information to. The Private Key is a closely-held key that allows a recipient to decrypt data that has been encrypted using the paired public key. A Private Key must be kept secret to preserve the security of a system of asymmetric encryption.

The term "backdoor" is an intentional vulnerability that companies leave in their systems so that outside actors, most oftenly the government, can decode encrypted information without the use of keys. Backdoors intentionally break encryption so they are favored by tech companies who devote much time and energy toward creating advanced encryption services. The Backdoor method is available so that companies are not directly offering sensitive information to the government without consulting with their consumers.

Challenges with Encryption

Increasingly in recent years, the Trump Administration has argued that encryption puts the government in a "Dark Age", limiting the national security, intelligence, and law enforcement communities' abilities to investigate threats or sensitive material, such as terrorist threats and child exploitation material. Technology companies condemn these uses, though most are willing to assist law enforcement with ongoing investigations or national security threats when requests to view certain data are made. Companies will work with investigators to provide example keys or code that allows them to view certain data. It can often be difficult to read the code that is provided, however, because it takes a particular skill set, training, or understanding in order for government officials to decipher keywords, phrases and programs of a given encryption. Not all software is the same and that's why encryption continues to work.

The alternative, and more commonly proposed idea, is that the companies using encryption allow a "backdoor" for the government to gain access to systems. This intentional vulnerability in the system allows the government or other actors to gain access. This would allow the government to view profiles, conversations, and information pertaining to criminal cases.

Governmental officials and investigators are forced to tackle an additional challenge in cases where devices or systems involve private encryption that is neither stored in a cloud, nor do companies have access to consumers' personally stored information. Equally, technology companies' hands become tied as they are forced to decide between providing uncontrolled access to the government and maintaining the privacy and security component that they supply users and customers.

Current Proposals and Legislation

While the government has the ability to wire-tap phone calls (CALEA Act 1994), it does not yet have the right to infiltrate information systems. There are a variety of proposals in Congress and the states to allow governmental access to encrypted information. One proposal from the National Security Agency would require technology companies creating a "split-key", which is essentially a digital key with separate pieces that could be held by different agencies as a "front door, not a back

door." This is simply another way to create vulnerabilities that decrease security in systems.

One bill currently circulating in Congress is the Eliminating Abusive and Rampant Neglect of Interactive Technologies ('EARN IT') Act, first introduced by Senator Lindsey Graham March of 2020. The bill would require tech companies to "earn" or be approved for Section 230 protections rather than be granted them by default, as the Communications Decency Act has ensured for more than twenty years. The intent of the bill is to "combat child sexual abuse material", but the bill would have lasting effects on all aspects of encryption and could decrease user confidence in technology privacy systems. The legislation would compel compliance from American technology companies but would not impact the encryption offerings from foreign companies or open source companies that are not subject to the same rules. If signed into law, many believe consumers would most likely lose trust in American technology systems and move to international systems that do not require governmental access. This would have lasting economic and social effects on the American technology industry, as well as innovation and development..

The Problem of Opening Doors

If a "backdoor" is created for the government to use, all individuals using the encryption program could face potential governmental supervision which could create a precedent of governmental invasion of privacy. Additionally, "backdoors" are not solely accessible to the U.S. Government. If the government is allowed a "backdoor", there is no certainty that only the government will be able to break such encryption, leaving gaps for bad actors to infiltrate platforms, businesses, and private conversations. This creates an overall vulnerability for systems and forces companies to invest in more encryption and security measures. "Backdoors" creates access tools, which are available to federal law enforcement and as well as foreign adversaries which undermines trust in the security of American technology offerings.

Major tech companies agree that the privacy and security component that encryption supplies users is what provides American tech businesses their value. If legislation forces American tech companies to loosen their encryption levels, users may look elsewhere in the world. Other countries will likely follow American legislation and as a result many countries, including authoritarian regimes will have access to users data and sensitive information from all around the world.

Conclusion

Encryption is a valuable tool in the world we live in. It provides both security of mind as well as protection of information. While there are situations where companies agree to help the government in investigations and secure the overall safety and wellbeing of the country, careful measures must be taken when it comes to the extent that encrypted information is made accessible. "Backdoors" create serious concerns when it comes to safety, protection, and privacy.. It is important to acknowledge the risks of creating a precedent of" backdoors" and free government decryption, and the threat of other actors wishing to obtain similar sensitive data and information.

Links to Other Resources

- Center for Democracy & Technology - Tech Talk: Apple's Erik Neuenschwander On Encryption & Society
- Charles Koch Institute - Nuts & Bolts of Encryption
- CIO - Compromised Encryption is a threat to National Security
- Congress.Gov - S.3398 EARN IT Act of 2020
- Defense 360 - Bad Idea : Encryption Backdoors
- EveryCRSReport.com - The Communications Assistance for Law Enforcement Act

- The Hill - What Coronavirus Reveals about Securing Encryption Backdoors
- Human Rights Watch- Why Encryption Back Doors Threaten Human Rights
- IRS - Encryption Requirements of Publication
- Just Security- Why an Encryption Backdoor for Just the "Good Guys" Won't Work
- Lawfare - Rethinking Encryption
- NS Tech- EARN IT: The US Bill That Could End All Encryption
- The New York Times- How Congress Can Vote Remotely
- The New York Times - Whose Side is Bill Barr On?