The Software Alliance

BSA

ENCRYPTION: Why It Matters

DATA IS INCREASINGLY CENTRAL to our personal lives, economic prosperity, and security. That data must be kept secure. Just as we lock our homes, restrict access to critical infrastructure, and protect our valuable business property in the physical world, we rely on encryption to keep cybercriminals from our data. Proposals to regulate this crucial form of protection — however well-intended — could weaken our security.

Software continues to spark unprecedented advances that transform the world around us. From life-saving medical breakthroughs, to safer transportation, to enabling global economic transformation, our lives are improving in countless ways through the ubiquity and utility of data powered by software.

Digital security is becoming increasingly important to protect us as we bank, as we shop, and as we communicate. And at the core of that security lies encryption. As our lives increasingly move online, everyone should be doing more to improve the digital security of data, not less. Our digital world is constantly under attack by cybercriminals:

Data breaches exposed at least 423 million identities in 2015 — increasing by more than 20 percent in just a single year.[1]

Americans worry about hacking — of their credit card information, phones and computers — more than any other crime.[2] And for good reason: nearly half of American adults have been hacked.[3]

[1] 2016 Internet Security Threat Report," Symantec, April 2016, https://www.symantec.com/security-center/threat-report

[2] "Hacking Tops List of Crimes Americans Worry About Most." Gallup, 2014. http://www.gallup.com/poll/ 178856/hacking-tops-list-crimes-americans-worry.aspx

[3] Pagliery, Jose. "Half of American adults hacked this year." *CNN Money*, 2014. http://money.cnn.com/ 2014/05/28/technology/security/hack-data-breach/

www.bsa.org/encryptionmatters

ENCRYPTION IN OUR DAILY LIVES

ENCRYPTION IS A PART of almost every service or device we use to live our lives online. Every day, often without us even being aware of it, encryption keeps our personal data private and secure. Encryption is a vault that secures our personal information that is held by businesses and government agencies. It is a lock that prevents identity thieves from stealing our information when we log on to our bank accounts. It is an extra layer of security to safeguard our critical infrastructures. And it is a secure envelope that keeps hackers from reading our personal communications. Encryption is all of these things and more:

Use of encryption continues to rise, with more than one-third of businesses in one recent survey reporting that their organization uses encryption extensively.[4]

Use of encryption is steadily shifting to a strategic activity, with organizations moving to an enterprise-wide encryption strategy.[5]

Government rules — around patient data, financial transactions, and consumer information — frequently require companies to encrypt the data they hold.

Securing the data at the heart of our modern economy is a never-ending effort tied to multiple, interconnected parties. This involves not just the software companies that create products and services but the consumers who rely on those products and services to power their daily lives, the companies that encrypt human resources, sales, or other data, and even the law enforcement officials who investigate crimes. With so many interests at stake, it is vital that discussions about the future of encryption involve all perspectives.

THE NEED FOR SMART PROPOSALS THAT KEEP US SECURE

RECENT GOVERNMENT ARGUMENTS that companies should weaken encryption will put consumers, and our security as a whole, at risk. Encryption that is deliberately compromised from the start by any built-in weaknesses is not effective encryption.

We deeply respect the needs of law enforcement and support their ability to access data — pursuant to lawful process — to keep us safe. But proposals to mandate developers build security flaws in their systems — such as requiring master keys or back doors so law enforcement can access encrypted data on people's personal devices — would actually weaken our defenses against cybercriminals and shake users' trust. Undercutting encryption in this way opens the door to bad actors and jeopardizes our privacy, online safety and security.

Encryption that is deliberately compromised from the start by any built-in weaknesses is not effective encryption.

The recent debate over encryption has focused almost entirely on one-half of the equation: demands by government that technology companies design their technology around law enforcement's need to access data. Not enough has been said about other available resources to fight crime or about how to improve law enforcement's cyberforensic and analytical resources and capabilities. To truly assist law enforcement in its mission to keep us safe, we must focus on both resources and capabilities.

Our digital world demands a new mindset that promotes safety and security. We cannot operate using outdated principles. Collectively, alongside law enforcement and government officials, we must develop smart solutions. The world is watching how the US addresses encryption and cybersecurity defenses, and we must seize this opportunity to craft and lead a new mindset.

[4] "2016 Global Encryption Trends Study." Thales and Ponemon Institute, 2016. https://www.thales-esecurity.com/company/press/news/2015/april/2015-global-encryption-and-key-management-trends-study-release

[5] Ibid