Encryption and "Exceptional Access"

Encryption is the technology that keeps the data on our phones, tablets, and other gadgets safe from unauthorized access. This mathematical process is all that stands between our most private data and criminals, identity thieves, or abusive partners. But law enforcement wants a way to bypass encryption without making it easier for these bad actors. **Unfortunately, a multitude of expert cryptographers have concluded that there's no feasible way to do this.**

In January 2018, FBI Director Christopher Wray publicly blamed the agency's failure to access information on 7,775 locked devices on encryption, even though law enforcement has many other timely, lawful avenues to access the data they need to do their jobs.

Meanwhile, a newly released audit of the San Bernardino case by the DOJ Office of Inspector General raised questions as to how forthright the FBI has been with Congress, the courts, and the American people. The OIG report also mentions that federal investigators contract regularly with outside researchers who work to provide access to encrypted devices. Indeed, recent reports indicate that law enforcement agencies are able to use commercial tools offered by companies like Cellebrite and Grayshift to unlock essentially any device on the market.

Encrypted Devices Provide Important Protections for Regular Consumers

Modern Americans carry their lives in digital format with them every day, on their phones, tablets, and laptops. Without encryption on their devices, all their personal, private data—from mobile banking accounts to social media logins to medical histories to emails and texts—can be copied from lost or stolen phones or laptops in seconds.

Encrypted storage on a device means that if the device is lost or stolen, the information on it is still difficult to access. **Encryption is all that protects data on lost and stolen devices.**

"Exceptional Access" for Law Enforcement Is "Open Access" for Other Bad Actors

There is no technological compromise between strong encryption that protects the data on Americans' devices and a mechanism to allow the FBI "exceptional access" to this data. Building an exceptional access mechanism on the vast scale needed to decrypt devices for law enforcement on a routine basis would put everyone at greater risk of hacking, identity theft, and fraud. In addition, any system implemented by the US government *will* be accessed and misused by repressive governments around the world, including against Americans.

Law enforcement asserts that encryption prevents them from doing their jobs. But, in light of the OIG report—and the availability of commercial unlocking tools—their claim is doubtful. **As both state-sponsored and criminal hacking tools get more sophisticated, strong encryption is even more important to keep consumers' financial and personal data safe.**

For more information, please contact India McKinney at india@eff.org