Breaking Encryption for Law Enforcement

Joshua Higgins & Alicia Wade

Encryption

Encryption provides an end to end protection of data, as well as what we call “data at rest.”

An encryption algorithm either encodes sensitive data or it doesn’t—the only method for allowing a third-party to gain access to plain-text data would be to either provide them with the private keys of the communicants in question or maintain an exploitable flaw in the algorithm that a third-party could take advantage of.

What Does Encryption Protect?

Encryption protects data at rest when stored on hard drives, cell phones, or in the cloud, and it can also protect data in transit as it moves from one device to another.

Encryption acts to protect the data, including personally identifying information, health information and financial information from being improperly used if intercepted.

What Does Law Enforcement Want?

Government/Law Enforcement insist that there should be a “backdoor,” or an access key into encrypted messages, and it should be enabled by private companies and shared with law enforcement agencies.

Governments have asked for both means of observing data in transit, as well as retrieving data at rest on devices of interest.

They also insist that they have no interest in weakening encryption as a whole, but just in retrieving the information they need for an investigation.

Cons (Banking and Businesses)

Economic Risks: modern digital economy relies on encryption for digital transactions and storage of sensitive information such as financial and medical information.

- Consumer protection, e.g. banks protecting financial information and stopping it being accessed or misused when people bank or make purchases online.

- Many businesses use end-to-end encrypted apps such as WhatsApp and other encrypted communications and VPNs. Encryption, therefore, protects sensitive company data, data privacy, and can reduce cybercrime risks.

Cons (National Security & National Relations)

Requiring exceptional access to encrypted technologies would undermine national security by:

- Weakening protections for the information that the national security community relies upon, especially as it flows over foreign networks.
- Creating a vulnerability in encrypted communications that could be accessed by foreign adversaries.
- Encouraging other countries to require tech and internet companies to provide equivalent access to communications within their boundaries.

Trade Agreement Repercussions: A country's decision to implement encryption regulations could have repercussions on existing trade agreements.

Cons (Disproportionate Impacts on Vulnerable Groups)

- Weakening encryption can have critical implications for many vulnerable groups. The confidentiality that encryption affords allows individuals and minority groups to associate freely, providing a safe environment for people seeking support or concerned that their communications may be subject to interference.
- Encryption helps protect the speech of vulnerable and marginalised communities who are more likely to be subjected to abuse, violence and discrimination because of their identity.

Cons (Communications During War)

- Providing reliable and safe communications in war situations, e.g. secure communication channels in Ukraine allowing broadcasted appeals to the world and recruiting support. Also, encryption has helped Ukrainians to combat disinformation, organise relief efforts, and protect evacuees.

  The first thing many Russian soldiers are reported to be doing when capturing people is to look at their phones to study their communications and track down associates. This is a good argument for encryption and features like disappearing messages sent via WhatsApp.

Cons

- **Protection for journalists** who need to keep information channels open despite government censorship.
- **State Abuse:** The Government is already using certain tracking software, but weakening encryption allows them to abuse their power, which can lead to **Loss of Consumer Trust.**
- **Limited Innovation and Choice:** protocols that have technical vulnerabilities intentionally introduced into them, say Free and open-source software, would not be adopted by organizations that want to build strong encrypted services.
- **Economic Impacts of Cybercrime:** Installing backdoors in encrypted systems creates technical vulnerabilities that could be exploited to commit cybercrime. This renders products and services that rely on encrypted systems vulnerable to cyber-attacks.

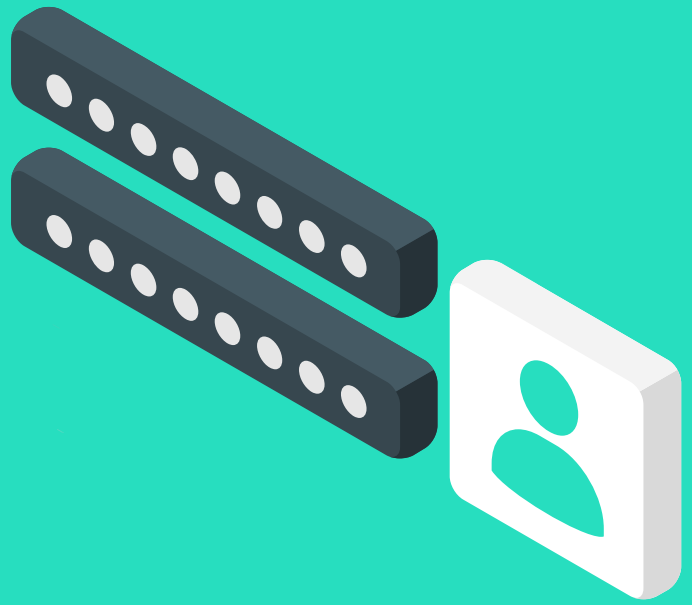
Background Information

In 2014 we had Riley v. California, which led to the requirement that law enforcement must have a warrant to search a suspect's phone upon arrest. This was an important decision, as upon arrest a suspect's body may be searched for incriminating evidence.

This rejection to the Fourth Amendment exception of unreasonable searches and seizures put cell phones on the same pedestal as home property (both of which require a warrant to search and/or seize information or things therein).

Pros

- Expedited access
- A decrease in government-funded cost



Further Background Information

In both they San Bernardino (2015) and Pensacola Naval Station (2019) shootings, law enforcement obtained warrants to search the devices and from there ran into a very well-known wall in their search for evidence: attempt limits.

The United States often relies on Grayshift and Cellebrite (both private companies) for these circumstances nowadays, each instance costing tens of thousands of dollars.

But in cases where suspects use rarer, or cutting-edge firmware or hardware it leads to a million dollar receipt.