Why we should not break encryption for law enforcement.

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.

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.
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.

Reasons for not breaking encryption:

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

- Requiring exceptional access to encrypted technologies would undermine national security.

- Weakening encryption can have critical implications for many vulnerable groups.

- Encryption helps protect the speech of vulnerable and marginalized communities.

- Providing reliable and safe communications in war situations, e.g. secure communication channels in Ukraine allowing broadcasted appeals to the world and recruiting support.

- 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.