

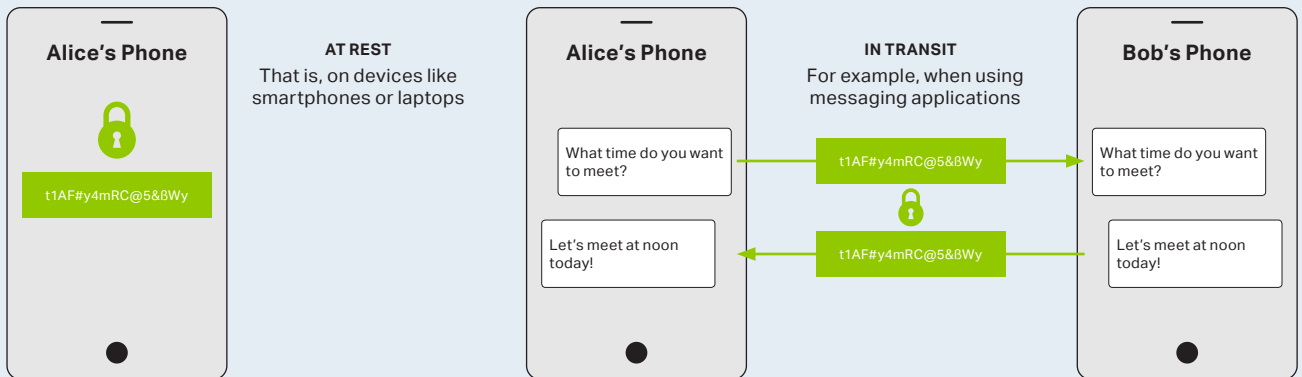
A Primer on Encryption and the Fuss About it

What is Encryption?

Encryption is the conversion of readable data ("plaintext") into scrambled data ("ciphertext"), making it unreadable without the correct key to decrypt the data. Encrypted data can be used to produce, for instance, private correspondence, credit card information, ID numbers, sensitive company information, or bank account information.

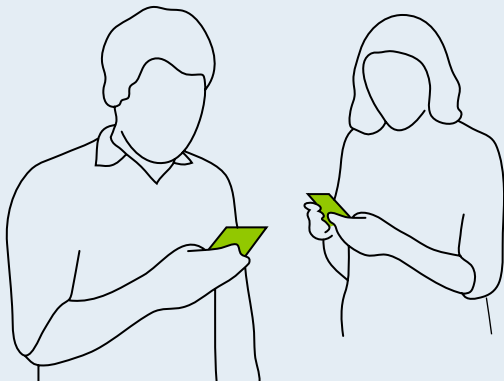


Where Does Encryption Take Place?



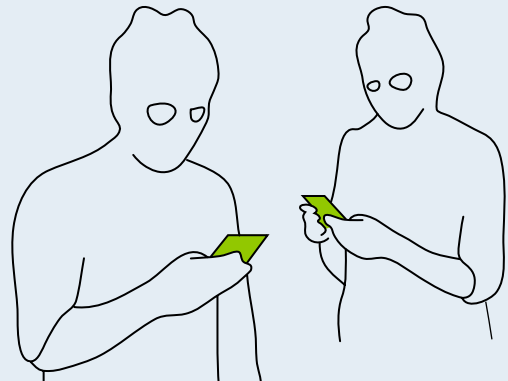
What is the Fuss?

The power of ciphers protects citizens when they read, bank, and shop online.



Bob: "Let's meet at noon today!"

But the power of ciphers also protects spies, terrorists, and criminals when they pry, plot, and steal.

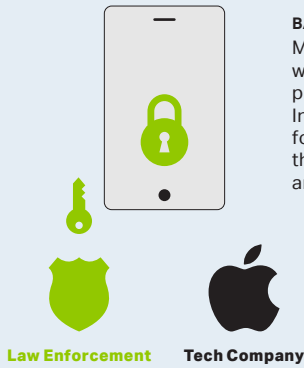


Bob: "Let's plot at noon today!"

...

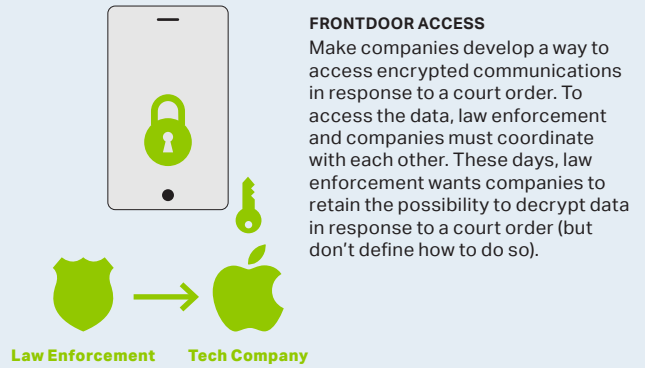
Law enforcement agencies argue that they are "going dark" in their investigatory efforts due to two trends: **(1) communication takes increasingly place online, and (2) companies are improving the security of technology through (default) encryption.** This increases the number of users, whose data becomes inaccessible.

What Do Law Enforcement Agencies Suggest?



BACKDOOR ACCESS
Make companies build products with a backdoor, or golden key, that permits access by law enforcement. In the 1990s, law enforcement asked for backdoor access that would give them direct access to data at rest and in transit.

Law Enforcement Tech Company



FRONTDOOR ACCESS
Make companies develop a way to access encrypted communications in response to a court order. To access the data, law enforcement and companies must coordinate with each other. These days, law enforcement wants companies to retain the possibility to decrypt data in response to a court order (but don't define how to do so).

Law Enforcement Tech Company

What Speaks Against Providing Lawful Access to Investigators?

NECESSITY
We do not know whether law enforcement is going dark. Opponents argue we live in a "golden age of surveillance" in which companies collect large amounts of data that investigators can use.



"Law enforcement can't read my messages, but it can figure out where I live, where I go, who my friends are, what I read, what I watch, and so on."

IMPLEMENTATION
National governments will struggle to regulate a global market for encryption technology, almost 50% of which is freely available online.

Availability of Encryption Technology



EXTERNALITIES
Regulation on encryption technology would have negative externalities. It would ...



Weaken IT security by creating additional vulnerabilities



Threaten the domestic tech industry by undermining trust in technology



Put human rights at risk globally, since authoritarian nations will follow with similar demands

What Are Other Proposals to Help Law Enforcement Get What They Want?

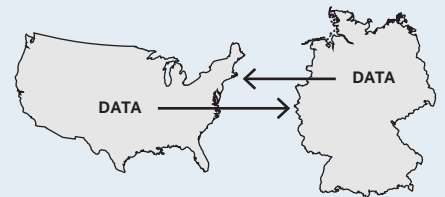
Form a lawful hacking regime that can get into devices when necessary.



Increase personnel, resources, and tech literacy.



Reform the system of international mutual legal assistance to better allow countries to exchange data while investigating crimes.



Another proposal is to collect content and metadata, i.e. data about data, via data localization and/or data retention in specific countries. In both cases, technical and legal concerns outweigh potential advantages.