OVERVIEW OF ENCRYPTION

THE DATA CHALLENGE

Technology such as computers, email, and personal devices have become storehouses, and access points to the internet and the cloud.
Technology companies are challengged are challenged to protect personal data and keep it private to particular users.

THE ROLE OF ENCRYPTION

Data encryption keeps your data more secure from third-parties trying to gather private information over public networks, unsecured accounts or devices, and through various methods to gain access to private accounts.

Password encryption protects your data, but decryption depends on the strength of your password.

A PERSPECTIVE ON END-TO-END ENCRYPTION

"End-to-end encryption is great for preventing companies and governments from accessing your messages. But for many people, companies and governments are not the biggest threat , and therefore end-to-end encryption might not be the biggest priority."

WHO WANTS YOUR DATA & HOW THEY ACCESS IT: THE TUG-OF-WAR FOR PRIVACY

WHO WANTS YOUR DATA?

THE GOVERNMENT
Desires to access protected data in the name of public safety and national security.

LAW ENFORCEMENT
Reports encrypted data impedes work (surveillance, terrorism, crimes). Wants technology companies to provide a "door".

PRIVATE-SECTOR COMPANIES
Uses gatekeeping power to collect personal data and sell to information resellers.

RANSOMWARE & HACKERS
Encrypts data and demands payment to unlock/release.

DATA FORTRESS

HOW DO ENTITIES ACCESS YOUR DATA?

LEGALLY
Warrants: Law enforcement needs probable cause for phone search, but "consent searches" are an exception.

CALEA: Requires telecom carriers to assist in surveillance (except encrypted data without key).

COMPANY PROVIDED "DOORS"
Backdoor/Front Door: Known vulnerability in OS to bypass security.

Tech Companies' Stance: Resistant due to exploitation risks and dangerous privacy precedents.

What is Encryption?

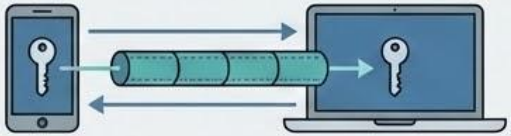
Encryption: Protecting Your Digital Life

"Encryption protects 'the privacy, security, and authenticity of information that is stored on a device or in the cloud or sent digitally.'"

It is the best technology we have to protect information from bad actors, governments, and service providers. When used correctly it is virtually impossible to break.

End-to-End Encryption

Encodes communications and data so that it can be read only by the person or system possessing the password, or "key" to decipher it.



Metadata is Not Protected

Encryption only protects the content of your communication, not the fact that you are communicating in the first place. It does not protect your metadata, which includes information like who you are communicating with and when.

Encrypting Data At Rest

Data "at rest" is data that is stored somewhere, like on a mobile device, laptop, server, or external hard drive. When data is at rest, it is not moving from one place to another.

Full-Disk Encryption (Device Encryption)

Encrypts all the information stored on a device and protects the information with a passphrase or another authentication method. Usually looks like a device lock screen, requiring a passcode, passphrase, or thumbprint. Locking your device does not always mean that full-disk encryption is enabled.

File Encryption

Encrypts only individual files on a computer or other storage device.

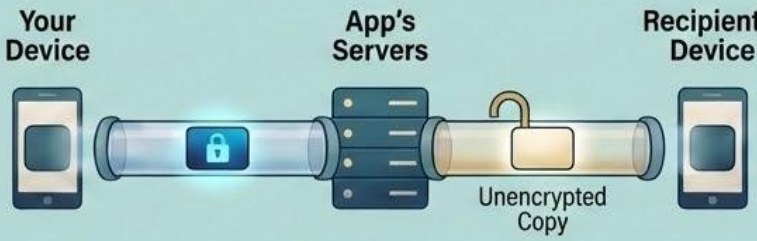
Drive Encryption (Disk Encryption)

Encrypts all of the data on a specific storage area on a device.

Encrypting Data In Transit

Data “in transit” is information that is moving over a network from one place to another.

Transport-Layer Encryption



Uses TLS protocol.
Messaging service providers can see unencrypted copies...
Vulnerable to law enforcement requests or leaks...

Examples:

HTTPS website servers can see data, but unreadable to eavesdroppers.

With VPN, traffic encrypted between you and VPN provider. Metadata is visible.

End-to-End Encryption

Protects messages all the way from sender to receiver.
Information is a secret message... decoded only by final recipient.
No one, including app servers, can "listen in" or eavesdrop.

What Encryption In Transit Does Not Do

Not a cure-all. Decrypted by the recipient.

If endpoints compromised, communications can be compromised.

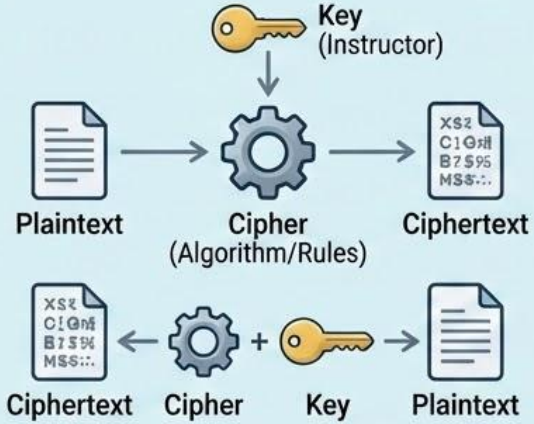
Recipient can take screenshots or keep records (logs).

Protects content, but will not encrypt metadata.

Key Concepts in Encryption

Ciphers and Keys: The Core Components

Encryption: Scrambling Information



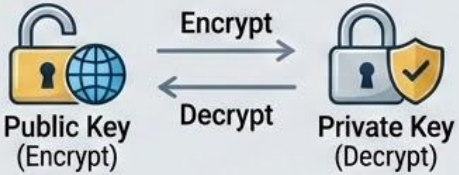
A mathematical process to scramble information, only decryptable with special knowledge. A cipher is a set of rules followed for encrypting and decrypting. A key instructs the cipher. Keys are crucial.

Symmetric & Asymmetric Encryption Methods

Symmetric Encryption (Single Key)

Widely used for files, full-disk, databases. Requires a password for decryption.

Asymmetric Encryption (Two Keys)



Involves two keys: Public for encryption, Private for decryption. Often used together with symmetric for data in transit.

Private and Public Keys: The Matched Pair

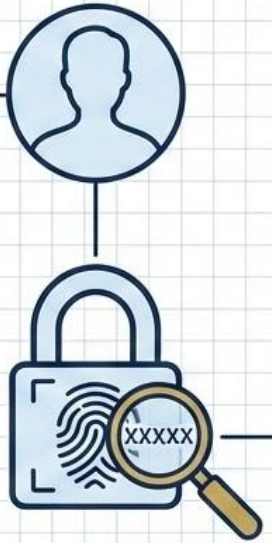
Come in matched pairs, mathematically tied together.

Both are needed for decryption.

Computer-readable representations of very large numbers.

Digital Identity & Security Verification: Methods & Alternatives

1. Identity Verification for People (Public Key Fingerprints)



Fingerprint Verification

A "Key fingerprint" is a string of characters to uniquely and securely check that someone on the internet is using the right private key.

2. Identity Verification for Websites (Security Certificates)

Browser makes encrypted connections using HTTPS

Modern browsers & OS include trusted Certificate Authorities (CAs) with pre-bundled public keys.

CAs sign the website's public key after validation.

Browser visits HTTPS site, verifies the certificate is signed by a trusted CA

Certificate Authorities (CAs)

A trusted third-party has verified the site's identity.

3. Alternative Methods (Access & Forensics)

Brute Force Attack

THWARTED

Auto-erase features erase all stored data after ten unsuccessful login attempts.

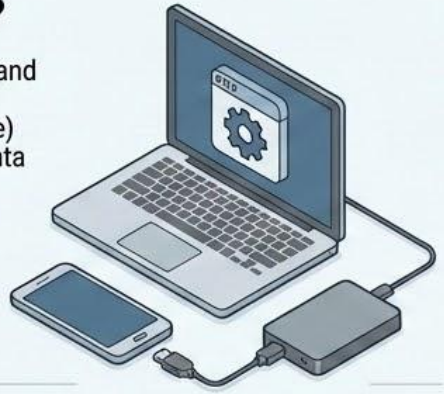
Cellphone Investigative Kiosks (CPIKs)

An FBI Regional Computer Forensic Laboratory tool to assist local law enforcement to extract data from a cellphone, put it into a report, and burn the report to a CD or DVD.

Mobile Device Forensic Tools (MDFTs): Capabilities and Scale of Use

1. What are MDFTs?

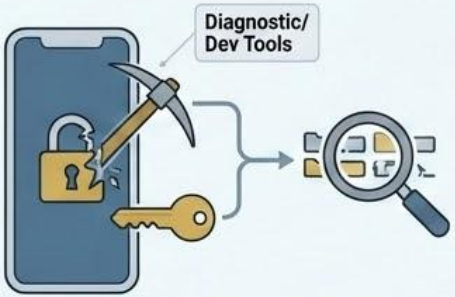
MDFT: a computer program and its supplemental equipment (e.g., cables, external storage) that can copy and analyze data from a cellphone or other mobile device.



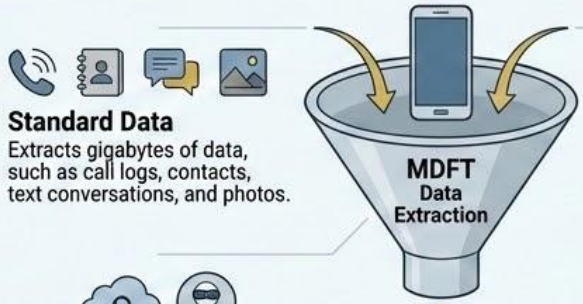
2. How They Work: Bypassing Security

May bypass a phone's security features by taking advantage of security flaws or built-in **diagnostic or development** tools to extract even encrypted data.

Can circumvent most security features in order to copy data.[31]



3. What Data is Extracted?



Standard Data
Extracts gigabytes of data, such as call logs, contacts, text conversations, and photos.

Deep Data & Artifacts
Extracts data from online accounts, third-party apps, "deleted" data, and even people's precise interactions with the device itself, which all leave behind artifacts, which MDFTs can find.

Cloud & Impersonation
Newer "cloud analyzer" tools, allow law enforcement to collect data from cloud storage or to impersonate the individual.

Analysis Interface
Makes it easy for law enforcement to analyze and search data copied from phones.

4. Scale of Law Enforcement Use

Law enforcement agencies have largely adopted MDFTs, with more than **2,000 agencies** across the United States (as of 2020) having purchased such products. Used for **hundreds of thousands of instances of data extraction** over a five year period, and in many cases with **no warrant**.

References

Communications Assistance for Law Enforcement Act, Pub. L. No 103-414, 108 Stat. 4297.
CRS Report R44187, Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations, by Kristin Finklea (2016).

Heather West, *Encryption: It's Not About Good and Bad Guys, It's About All of Us*, Ctr. for European Pol'y Analysis (Dec. 5, 2023), https://cepa.org/comprehensive-reports/encryption-its-not-about-good-and-bad-guys-its-about-all-of-us/.

Jack Nicas, *The Police Can Probably Break Into Your Phone*, *N.Y. Times* (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html.

Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, 27-28, Upturn (Oct. 2020) ("In April 2018, Professor Matthew Green estimated that brute-forcing a passcode on an iPhone would take no more than 13 minutes for a 4-digit passcode, 22 hours for 6 digits, and 92 days for 8 digits").

Nolan Goldberg & Anisha Shenai-Khatkhate, *Ransomware Planning and Response Best Practices*, Lexis+ (database updated May 2, 2025), https://plus.lexis.com/api/permalink/253ced19-ffa6-4bf4-afc6-5be268e0f332/?context=1530671.

Tracey M. DiLascio, *Data Encryption and Law Enforcement Investigation: Overview*, EBSCO Research Starters (2024), https://www.ebsco.com/research-starters/law/data-encryption-and-law-enforcement-investigation-overview#full-article.

U.S. Gov't Accountability Off., GAO-13-663, 2-4, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* (2013), https://www.gao.gov/assets/gao-13-663.pdf#page=5.62 (last visited Feb. 2, 2026).

Surveillance Self-Defense, *Key Concepts in Encryption*, Electronic Frontier Found. (Jan. 1, 2025), https://ssd.eff.org/module/key-concepts-encryption.

Surveillance Self-Defense, *What Should I Know About Encryption?*, Electronic Frontier Found. (Jan. 1, 2025), https://ssd.eff.org/module/what-should-i-know-about-encryption.

This document offers guidance to help individuals protect their digital hygiene. But self-protection is not a panacea—lasting safety depends on stronger legal protections as well.

To learn more about the proposed New York Privacy Amendment and the policy landscape around digital privacy, contact Jared Trujillo at jared@equalityny.org.