How the cops can get your data

Laws that permit access to user information

Presented by: Aaron Mackey & Saira Hussain

ELECTRONIC FRONTIER FOUNDATION

EFF is an international nonprofit that champions user privacy, free expression, government transparency, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.

EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

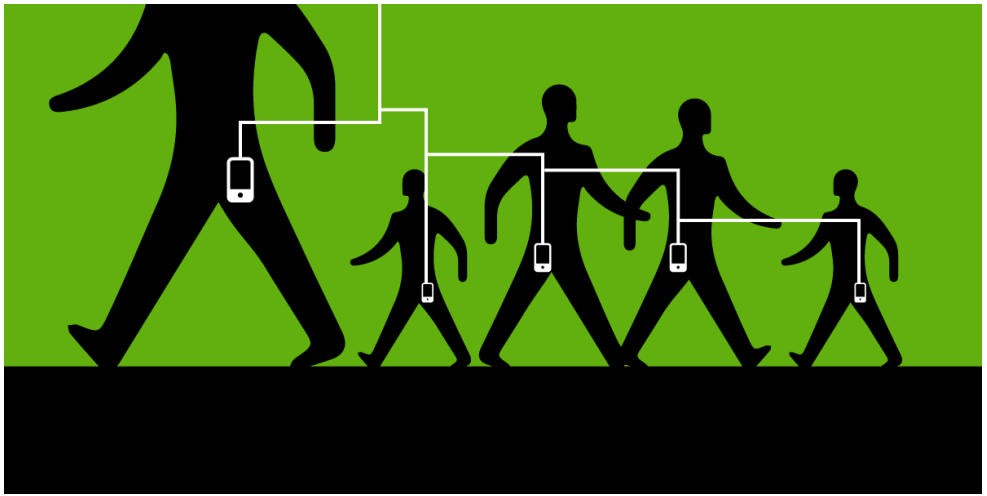
More about EFF

- Goal: ensure that rights and freedoms are enhanced and protected worldwide as our use of technology grows
- Tools: Litigation, Activism, Technology
- Details
  - Community supported
  - About 100 staffers
  - Based in San Francisco
  - Founded in 1990

EFF's anti-surveillance work

EFF brings lawsuits or files amicus briefs in cases to protect individual's Fourth and Fifth Amendment rights, including:

- *Carpenter v. U.S.*, 585 U.S. 296 (2018) (established warrant requirement for police to obtain cell-site location information) (cited by court)
- *Simon v. San Francisco* (9th Cir. 2024) (challenge to electronic monitoring of people on pre-trial release)
- *Armendariz v. Colorado Springs* (10th Cir. 2024) (challenge to dragnet device searches of protester)



April 30, 2025

Can the cops get my data?

Short answer: YES!

A variety of federal and state laws give law enforcement powers to obtain lots of different information about the online services we use to communicate.

We'll provide an overview of how this can work.

Legal demands

An overview

Types of data police can access

- Customer/subscriber information
- Transactional/metadata about communications
- Contents of communications

How police can access the data

- Retrospective/stored
- Interception/wiretap
- Prospective

Legal demands

An overview

Common methods to demand data

- Subpoena
- Court order
- Search warrant

Other considerations

- Gag orders on providers
- National Security laws
- How services can push back or stand up for users' rights

Important caveats!

This is not legal advice – if you have specific issues and needs, talk with a lawyer.

This is not threat modeling – not a substitute for comprehensive, nuanced thinking about the sorts of protections you want for data against specific adversaries.

Laws generally provide greater protection for more sensitive data

Type of data	Process used	Proof needed	Provider/user challenge before disclosure?
Subscriber information (information you provided at sign up, when you signed up)	Subpoena	Relevant to an investigation	Yes
Non-content such as transaction logs and other metadata	Court order; though sometimes a subpoena (lines are blurry)	Specific and articulable facts that info is relevant to investigation	Yes
Stored content	Search warrant	Probable cause that info will provide evidence of a crime	No
Intercepting content in transit	Super warrant	Probable cause plus exhaustion, and minimization	No

Laws generally provide greater protection for more sensitive data

Type of data	Process used	Proof needed
Subscriber information (information you provided at sign up, when you signed up)	Subpoena	Relevant to an investigation
Non-content such as transaction logs and other metadata	Court order; though sometimes a subpoena (lines are blurry)	Specific and articulable facts that info is relevant to investigation
Stored content	Search warrant	Probable cause that info will provide evidence of a crime
Intercepting content in transit	Super warrant	Probable cause plus exhaustion, and minimization

As requests seek information that is closer to the content of communications, law enforcement has greater factual and legal burden to compel disclosure

But – that does not mean cops won't try an end run!

Type of data	Process used	Proof needed
Subscriber information (information you provided at sign up, when you signed up)	Subpoena	Relevant to an investigation
Non-content such as transaction logs and other metadata	Court order; though sometimes a subpoena (lines are blurry)	Specific and articulable facts that info is relevant to investigation
Stored content	Search warrant	Probable cause that info will provide evidence of a crime
Intercepting content in transit	Super warrant	Probable cause plus exhaustion, and minimization

Law enforcement sometimes asks for more than what they are legally permitted to, i.e. using a subpoena to demand the contents of communications.

Remember: if seeking content, tell cops to come back with a warrant.

Pay close attention to the scope of what the process seeks

Type of data	Process used	Proof needed
Subscriber information (information you provided at sign up, when you signed up)	Subpoena	Relevant to an investigation
Non-content such as transaction logs and other metadata	Court order; though sometimes a subpoena (lines are blurry)	Specific and articulable facts that info is relevant to investigation
Stored content	Search warrant	Probable cause that info will provide evidence of a crime
Intercepting content in transit	Super warrant	Probable cause plus exhaustion, and minimization

These processes also have basic minimum requirements.

E.g. Search warrants require particularity, so a warrant that allows for an unbounded search of stored content should be a red flag.

When provider/user can challenge depends on process used

Type of data	Process used	Provider/user challenge before disclosure?
Subscriber information (information you provided at sign up, when you signed up)	Subpoena	Yes
Non-content such as transaction logs and other metadata	Court order; though sometimes a subpoena (lines are blurry)	Yes
Stored content	Search warrant	No
Intercepting content in transit	Super warrant	No

Subpoenas and court orders can usually be challenged prior to the disclosure of data. Search warrants and wiretaps usually cannot be.

User notice and challenges to legal demands

Best practices for service providers: Notify users that law enforcement has sought their data and give them opportunity to find a lawyer to fight.

Bonus points: provider challenges legal demand themselves.

But! Sometimes law enforcement obtain gag order (non-disclosure order) preventing provider from giving notice to targeted users.

Best practices

Law enforcement cannot compel disclosure of data that the service or the user do not have.

Services should:

- Collect only minimum info necessary to provide service.
- Consider whether you a need to continue to keep various types of user data or whether it can be deleted.
- Develop robust retention/deletion schedules (seek legal help before implementing).

Best practices

Law enforcement cannot compel disclosure of data that the service or the user do not have.

Users should:

- Consider deleting data from services when it's no longer needed.
- Evaluate data collection/retention and user notice practices of services before using them.

Myths that won't die but should

Just because data is stored abroad or service provider is based outside the United States, it is not beyond the reach of United States, state, and local law enforcement.

There is no "one neat trick" to avoiding law enforcement demands. Often the provider storing the data is based in the U.S. or has an agent responding to legal demands if they are outside the country. And if not, there are ways for U.S. law enforcement to obtain data stored in other countries by non-U.S. services.

Myths that won’t die but should

A service provider can always protect my data in the face of law enforcement demands.

Service providers that push back in court can sometimes have success. But they are not always successful and still must follow the law. Do not assume that a provider can ignore or otherwise not comply with a legal demand.

Questions?