Stanford University

Intro to the U.S. Legal System, Privacy, Surveillance & Law Enforcement

Riana Pfefferkorn
Policy Fellow, Stanford HAI

CS 152: Trust & Safety

April 14, 2026

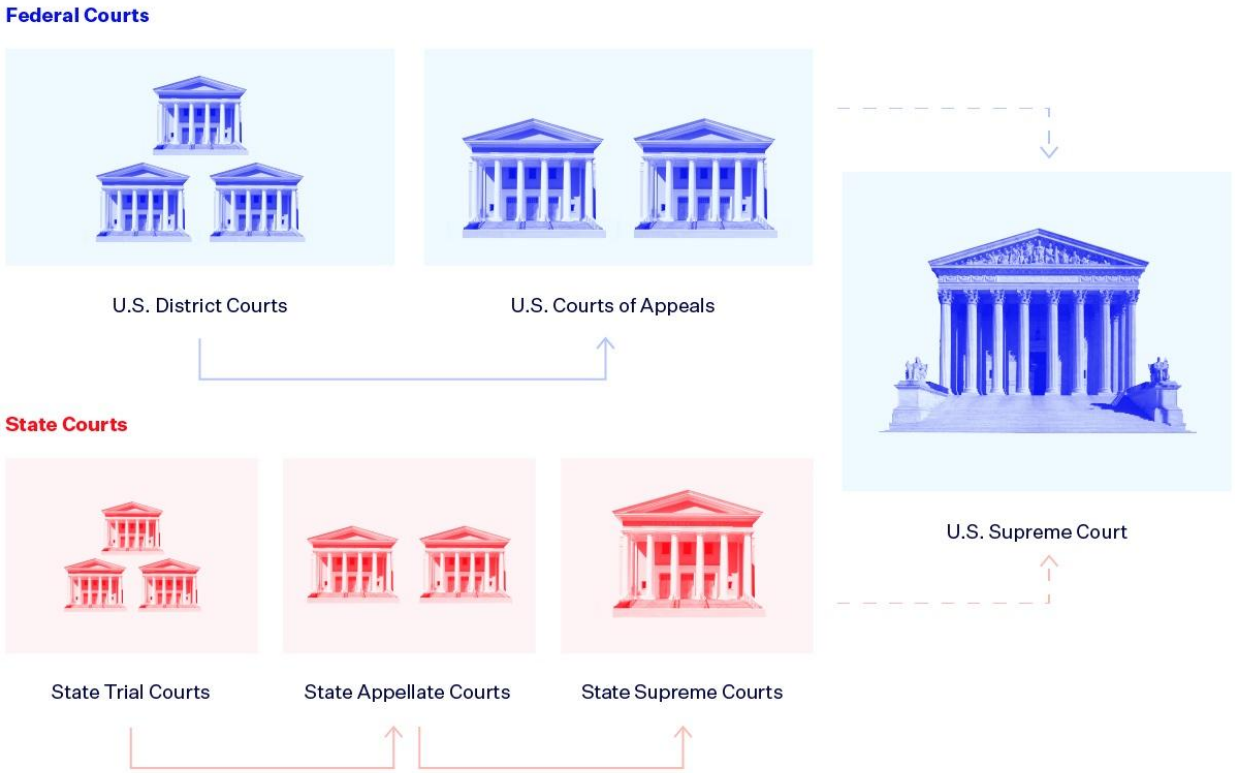
U.S. Legal System Overview

Stanford University

Sources of law (federal and state)

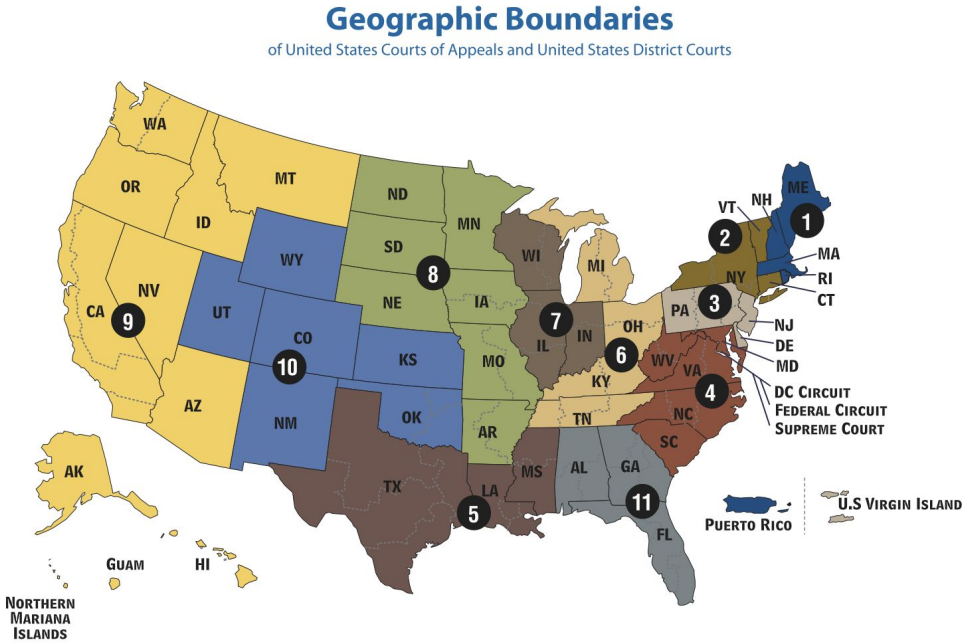
- Constitution
- International: treaties & executive agreements
  - Example: Budapest Convention on Cybercrime
- **"Statutory law":** Legislative branch
  - Statutes enacted by the legislature
- **"Administrative law":** Executive branch
  - Agency rules (aka regulations)
    - In addition to rules, look at orders in agency's cases, other guidance docs
  - Executive orders (President or state governor)
- **"Case law":** Judicial branch
  - Judicial opinions
    - Court levels: trial (lowest), appeals (intermediate), supreme (highest)
    - "Binding" versus "persuasive" precedent

The U.S. dual court system: federal and state



Source

Map of the federal court system



Source

Federal law

By American Broadcasting Company - A screen shot from “I’m Just a Bill”., Fair use, https://en.wikipedia.org/w/index.php?curid=62824163

Where federal laws live: United States Code (U.S.C.)

U.S. Code
→ Title
→ Subtitle (sometimes)
→ Part (sometimes)
→ Chapter
→ Subchapter > Part (sometimes)
→ Section

Source

How do the police get hold of your DMs?

Basics of the Fourth Amendment and federal communications privacy law

Stanford University

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable** searches and seizures, shall not be violated, and no Warrants shall issue, but upon **probable cause**, **supported** by Oath or affirmation, and **particularly** describing the place to be searched, and the persons or things to be seized.

Pre-ECPA Supreme Court cases

- 4A protects conversations from warrantless surveillance.
  - **In-person conversations:** *Berger v. New York*, 388 U.S. 41 (1967)
  - **Phone calls:** *Katz v. United States*, 389 U.S. 347 (1967)
    - 4A protects **people**, not just places, against unreasonable search & seizure
    - Concurring opinion: "reasonable expectation of privacy" test → still the touchstone for courts' 4A analysis today

Third Party Doctrine

- But, 4A doesn't protect *phone numbers* held by third parties, nor information you *disclose* to third parties (business records).
  - *Smith v. Maryland*, 442 U.S. 735 (1979) (installation of a "pen register" at phone company, which collected phone #s the suspect dialed, wasn't a 4A "search")
  - *United States v. Miller*, 425 U.S. 435 (1976) (bank records not protected by 4A)
- Doctrine limited by *Carpenter v. United States*, 585 U.S. 296 (2018)
  - Warrant required to obtain 7+ days of historical cell site location info, even though subscriber "voluntarily" disclosed that info to the carrier
  - One of several "digital is different" 4A decisions by SCOTUS
- 4/27: SCOTUS oral argument in *Chatrie* (4A & "geofence" warrants)

Congress's response to SCOTUS 4A rulings

- In 1968, after *Berger* & *Katz*, Congress passed original Wiretap Act
- In 1986, after *Miller* & *Smith*, Congress passed ECPA
  - Amended the **Wiretap Act** (now Title I of ECPA), 18 U.S.C. § 2510 *et seq.* – **prospective**; applies to real-time interceptions of contents of communications; extended to include transmissions of electronic data via computers
  - Added the **Stored Communications Act** (Title II of ECPA), 18 U.S.C. § 2701 *et seq.* – **historical**; applies to stored electronic communications
  - Added the **Pen Register Statute** (Title III of ECPA), 18 U.S.C. § 3121 *et seq.* – **prospective**; applies to transactional info about wire & electronic communications

Disclosure of user data to governments

ECPA governs tech companies' **voluntary** and **compelled** disclosures of their users' **communications content** and **non-content data**.

When a **government** requests user data from a company, the company's response will depend on:

- the **type of data sought**,
- whether the data is **historical** or **prospective**,
- whether the requester is a **domestic** or **foreign government**, and
- what type of **legal process** (if any) the requester uses to request the data.

Metadata → company can disclose to domestic government (with a **subpoena**) or foreign government (if the company **voluntarily** chooses; can't be compelled)

- E.g. **"basic subscriber information" (BSI)** such as name, address, IP address, login history

Contents of user's stored communications → disclosure requires a **warrant** issued by a domestic court

- **Mutual legal assistance treaties (MLATs):** foreign govt requests go thru DOJ, which presents them to a federal judge. Must meet US standards (e.g. "probable cause")
- Countries with **CLOUD Act** agreements with the US can bypass MLAT and serve user data requests directly on the company (so far, only UK, Australia)

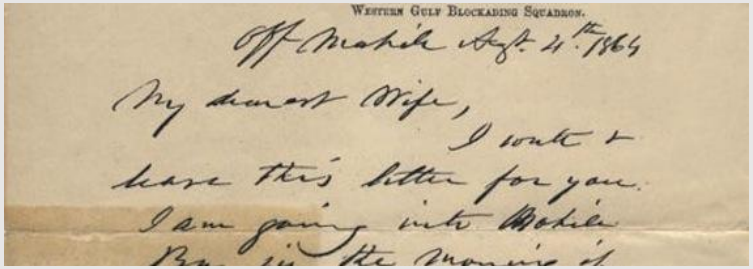
Contents of communications as they're sent → interception requires a **wiretap order** issued by a federal district judge (aka "Title III order" or "superwarrant")

- MLATs & CLOUD Act do not cover wiretaps

Content/non-content distinction

Contents = "**substance, purport, or meaning**" of the communication

- What the communication conveys
- Example: email subject line + body

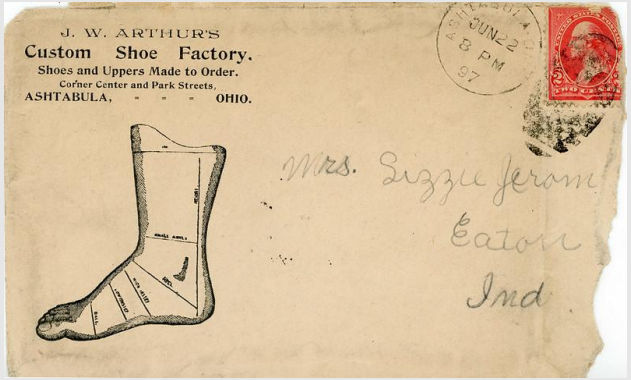


Source

Non-content information = information **about** the communication

- "Metadata"
- Example: header of an email

(This distinction can get blurry in the digital age)



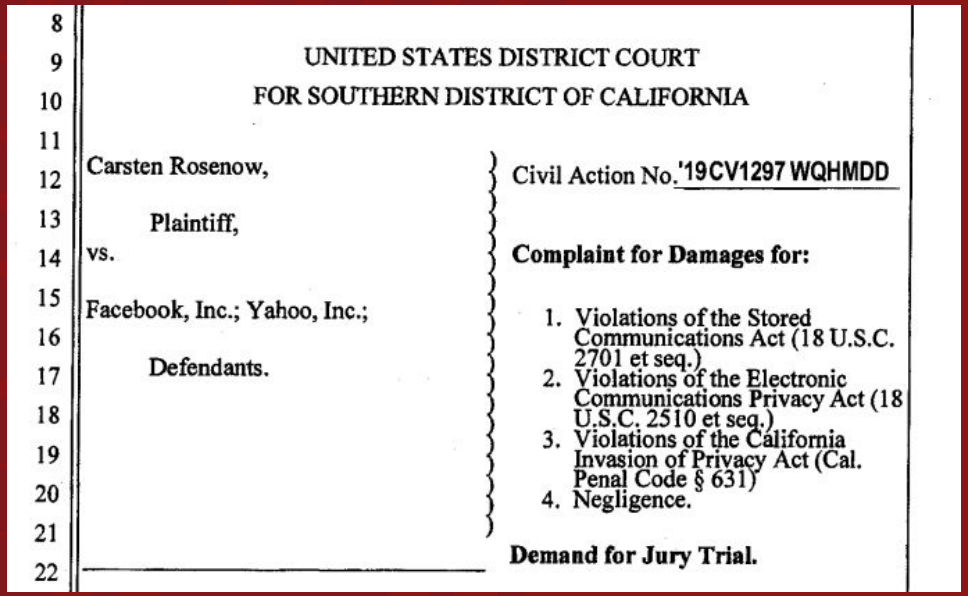
Source

Stored Communications Act: Who Can Get What, How

	Governmental entity (e.g. fed/state prosecutor)	Non-governmental entity (e.g. civil litigant, criminal defendant)
Basic Subscriber Information (see 18 U.S.C. § 2702(c)(2))	• Federal, state, or local administrative, grand jury, or trial subpoena • Court order issued under SCA section 2703(d) • Federal or state search warrant	• Federal or state court civil or criminal defense subpoena or court order • (Foreign government requests require domesticated order) (or a CLOUD Act agreement)
Other non-content records or information	• Court order issued under SCA section 2703(d) • Federal or state search warrant (*Carpenter*: 7+ days of historical cell site location info)	
Contents of communications	• Federal or state search warrant	• No means to compel; must seek it from the user (but case law saying that a subpoena + consent can compel content)

(CA state courts have been messing this up)

Source: adapted from Perkins Coie



UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF CALIFORNIA

Carsten Rosenow,

Plaintiff,

vs.

Facebook, Inc.; Yahoo, Inc.;

Defendants.

Civil Action No. '19CV1297 WQHMDD

Complaint for Damages for:

1. Violations of the Stored Communications Act (18 U.S.C. 2701 et seq.)
2. Violations of the Electronic Communications Privacy Act (18 U.S.C. 2510 et seq.)
3. Violations of the California Invasion of Privacy Act (Cal. Penal Code § 631)
4. Negligence.

Demand for Jury Trial.

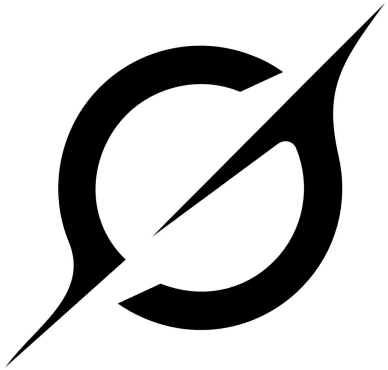
ECPA permits civil liability against a provider for violating ECPA's rules about disclosing user info

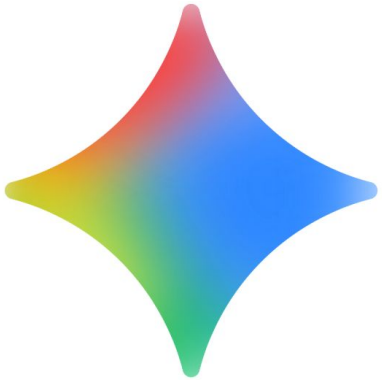
(but provider can invoke the defense of good-faith reliance on court orders, warrants, grand jury subpoenas, other reasons specified)

word of the day:
dog

Current topics in digital communications privacy

Government demands to AI companies





Sources: ChatGPT, Claude, Gemini, Grok

Salgado & Pell, *Installing a Content Patch in the SCA* (March 2026)

"Congress defined the term 'electronic communication' broadly. Information can constitute an electronic communication even if there is no second party or communicant; a user uploading data for their own use qualifies. The term does not require the involvement of some 'other' from whom it is sent or to whom it is conveyed. Congress knew that the enormous value of developing digital services included users uploading data for their own purpose of storage for later access, or for processing. Thus **a search query or prompt to be processed by an AI service for text or image generation are 'contents of an electronic communication' for the purpose of the SCA**."

(pp. 11-12, cleaned up, emphasis added) (link to paper)

Warrant to xAI for Grok prompts

- Stalking case involving harassing messages, SWATting, etc.
- Search warrant executed at suspect's home
- Devices seized; suspect admits during interview to using AI
- FBI review of seized Chromebook's browser histories reveals searches for Grok
- FBI issues search warrant to xAI (which is still sealed)
- xAI warrant return includes prompts to Grok

OpenAI warrant affidavit

- **Probable cause & particularity:**
  - Recites factual basis tying sought-after ChatGPT user account to the suspect user allegedly running CSAM sites
  - Request limited to "two unique, specific prompts … and the unique responses," made on specific dates
  - Affidavit devotes 5 pages to lengthy ChatGPT responses → very unlikely to match >1 ChatGPT user account

headquartered at 3180 18th Street, San Francisco, California. Specifically, this warrant seeks records and information pertaining to two unique, specific prompts made to OpenAI's "ChatGPT" program by a SUSPECT USER and the unique responses generated by ChatGPT.[…]

17. On several occasions in private conversations on the dark web between the UC and SUSPECT USER, the SUSPECT USER has told the UC about using ChatGPT. More specifically on April 18, 2025, the SUSPECT USER indicated SUSPECT USER had created/submitted the prompt to ChatGPT[6]: *what would happen if sherlock holmes met q from star trek?*

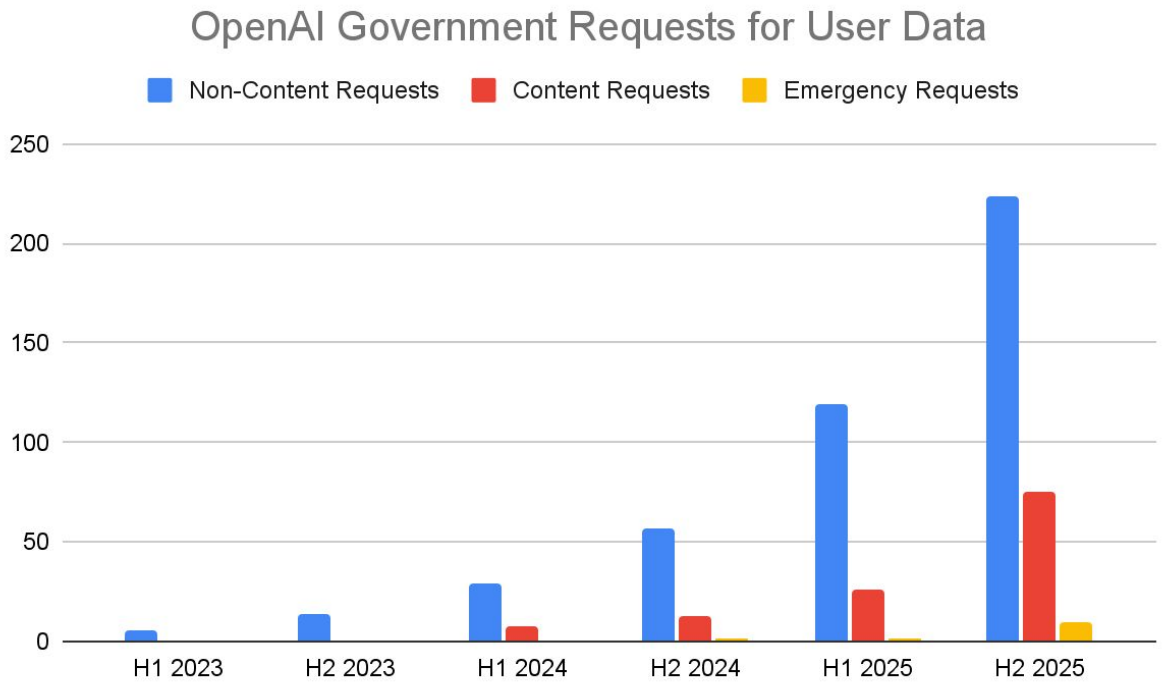
18. SUSPECT USER told the UC that SUSPECT USER received the response: *If Sherlock Holmes, the legendary detective, were to meet Q, the omnipotent, mischievous being from Star Trek, it would be an intriguing collision of intellect, wit, and power. Here's how it could play out:* […]

19. Additionally on April 29, 2025, the SUSPECT USER and the UC were engaged in a direct message conversation on the dark web. During the conversation, the SUSPECT USER indicated to the UC that SUSPECT USER had received the following response from ChatGPT, but did not specify the prompt that had been entered into the program: *Writing a 200,000-word poem is a massive undertaking — longer than most novels! To give you something useful, I can create a sample excerpt of a humorous, Trump-style poem about his love for the Village People's "Y.M.C.A.", written in that over-the-top, self-aggrandizing, stream-of-consciousness style he's known for. Here's a short sample to start — let me know if you want more added in parts!* […]

My questions about the OpenAI warrant

- Will judges be willing to OK reverse prompt warrants, like they did geofence/keyword?
- For reverse prompt warrants that push the envelope, will prosecutors "judge-shop"?
- How powerful is OpenAI's search capability for prompts/responses in chat histories? (How far back can they go, technical burden, free vs. $ plans, etc.)
- How will OpenAI respond if a demand corresponds to multiple unspecified users?
- How will OpenAI respond to warrants re: 1A-protected activity, abortion, GAC, etc.?
- How do Altman's ties to the USG affect OpenAI's response to legal process from USG?
- Has OpenAI ever received a gag order, fought to lift one, or moved to quash a warrant?
- What changes would render OpenAI unable to comply with a reverse prompt warrant?

So far, OpenAI rarely gets asked for user data



(data source)

Foreign Intelligence Surveillance Act (FISA)

- Section 702 of FISA permits USG to intercept comms of foreigners located abroad
- But we *in* the U.S. often talk to people *outside* U.S. → USG collects huge quantities of comms of U.S. citizens, LPRs, others on U.S. soil
- "Backdoor searches": FBI warrantlessly reads Americans' private messages collected under 702 → ruled unconstitutional in 2024 by NY federal district judge
- Section 702 periodically requires congressional reauthorization; in 2024, Congress passed a 2-year extension that expires **next week**; House to consider 18-month extension **tomorrow**
- FISC (FISA court) recently renewed its approval of the 702 program (which comes up annually), so it can continue through March 2027 even if Congress lets its auth expire
- Bipartisan bill was introduced in Congress last month to overhaul FISA & require a warrant for backdoor searches, but has gone nowhere yet (unsurprising: Congress prefers to bow to national security concerns, reauth 702, & kick the can down the road for the next Congress)

Thank You