Digital Evidence and the Law Update

MAJ ReAnne Wentz
Senior Defense Counsel
reanne.r.wentz.mil@army.mil

Google, ChatGPT, and your Phone Know All Your Things

MAJ ReAnne Wentz
Senior Defense Counsel
reanne.r.wentz.mil@army.mil

Digital Evidence Affects All Areas of MJ

- Investigation (4th and 5th Amendment – private search doctrine, third party doctrine, staleness, particularity, etc.)
- Charging (AI-generated CSAM, deepfakes, communication of indecent language)
- Discovery (See *United States v. Secord*, *United States v. Braum*, preservation)
- Trial (AI, authentication, trial prep, professional responsibility)

Agenda

- Geofencing
- Reverse Keyword Searches
- AI
- Border Searches

Geofencing


Geofencing

Google Just Killed Warrants That Give Police Access To Location Data

"Geofence warrants," which allow law enforcement to get location data across a wide area, have become commonplace in recent years.

Cyrus Farivar Forbes Staff

I'm a senior writer covering everything from scams to surveillance.

Thomas Brewster Forbes Staff

Senior writer at Forbes covering cybercrime, privacy and surveillance.

Dec 14, 2023, 05:43pm EST

What is Geofencing

- Using RFID, Wi-Fi, Bluetooth, cell data, etc. to track when someone enters or exits a perimeter
- Used by companies

  Uber

  Target

  Starbucks

  Chik-fil-A
- Used by law enforcement to search where a crime occurred

United States v. Rhine

- January 6 Rioter
- PC to arrest based on: geofence warrant information, two tips related to Rhine, surveillance footage from inside the Capitol, and CSLI.

  Geofence warrant shows that Rhine was present in 26 points – 22 within the Capitol itself.
- Rhine argued the geofence warrant was overbroad and lacked particularity


Robert A. Taft Memorial and Carillon
Senator Robert P. Casey Jr.
Senator Mitch McConnell
Ulysses S. Grant Memorial
Department of the Interior
Capitol Visitor Center
Rayburn House Office Building Extension
Independence Avenue SW
Constitution Avenue NW
Pennsylvania Avenue NW
Madison Drive NW
Jefferson Drive SW
3rd St SW
1st St SW
12th St SW
14th St SW

Three Step Process

- Identify all devices. This led to a total of 5,723 devices.
- List of devices that were present at the capitol between 12:00 – 12:15 p.m. and 9:00 – 9:15 p.m. This led to a total of **5,518** devices.
- Subscriber information for two groups of users: those entirely within the geofence and any devices for which the location history was deleted between Jan. 6 and Jan. 13. This led to details for **1,535** users.

Circuit Split

United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025)

- Robbery. Geofence had a diameter of 300 meters (longer than three football fields)
- Affirmed the district court's denial of Chatrie's suppression motion.

United States v. Smith, 110 F.4th 817 (5th Cir. 2024)

- Robbery. Geofence covered 98 square meters; 5:00 – 6:00 p.m.
- The Third-Party Doctrine did not apply and, therefore, the two appellants had a reasonable expectation of privacy

Reverse Keyword Searches

Search Google or type a URL

Mail

JAGCNet Ho...

EAMS

Google Maps

Privacy

Defense Trav...

Reverse Keyword Searches

- LE asks Google to provide information relating to specific searched terms or words
- Still a multi-step process

Colorado v. Seymour

536 P.3d 1260 (Colo. 2023)

- Arson. LE at a dead end. "[I]nvestigators surmised that the perpetrators had intentionally targeted the address. In pursuing this theory, they inferred that the perpetrators would have researched the property before burning it down or, at the very least looked up directions to get there."
- LE asked Google to ID users who had searched the address within a specified period.

Pennsylvania v. Kurtz

348 A.3d 133 (Pa. 2025)

- Facts: In July, 2016, K.M. sexually assaulted in her house while her husband was working an overnight shift. Unknown assailant.
- Police obtained a search warrant directed at Google for records of searches made with Google search engine for the victim's name or home address for the week preceding the July 2016 incident. Google returned a report that identified an IP address as having conducted two searches of K.M.'s address several hours before the attack. The IP address belonged to Kurtz.
- Court relies on Third Party Doctrine

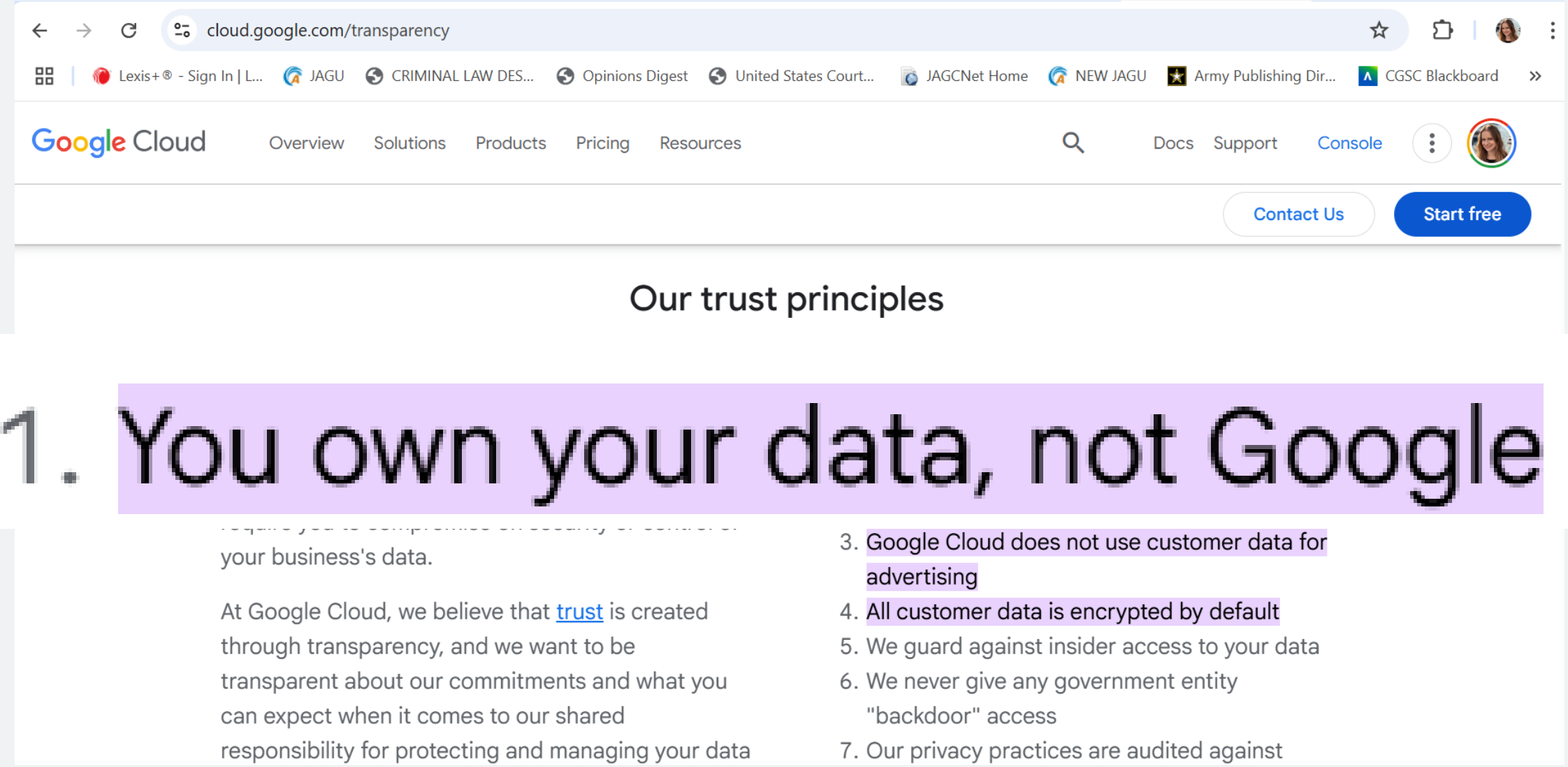
CrimPro Refresher

Katz v. United States, 389 U.S. 347 (1967)

- Subjective expectation of privacy
- Objective expectation of privacy, that is, one that society is prepared to recognize as reasonable

Smith v. Maryland, 442 U.S. 735 (1979)

- "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."
- Third Party Doctrine


cloud.google.com/transparency
Lexis+® - Sign In | L...
JAGU
CRIMINAL LAW DES...
Opinions Digest
United States Court...
JAGCNet Home
NEW JAGU
Army Publishing Dir...
CGSC Blackboard
Google Cloud
Overview
Solutions
Products
Pricing
Resources
Docs
Support
Console
Contact Us
Start free
Our trust principles
1. You own your data, not Google
your business's data.
At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data
3. Google Cloud does not use customer data for advertising
4. All customer data is encrypted by default
5. We guard against insider access to your data
6. We never give any government entity "backdoor" access
7. Our privacy practices are audited against

Key Findings:

- 56% of AI users have asked AI for legal advice.
- 50% of AI users were unaware that their ChatGPT conversations could be subpoenaed as evidence in court.
- 67% of AI users believe AI conversations should have the same legal protections as conversations with lawyers or doctors.
- 51% of AI users would be much more likely to consult a human lawyer instead of ChatGPT if they knew AI conversations could be subpoenaed.
- 76% of AI users think the government should regulate AI companies to provide legal privilege for user conversations.
- 47% of AI users think there should be prominent warnings before each conversation to inform users about potential legal risks.

machine learns from data instead of being explicitly programmed for every single rule.

- A **Large Language Model (LLM)** is a *specific type* of ML, like an **Electric SUV**. It's a highly advanced, specialized type of "car" designed specifically to understand, generate, and work with human language.

Here is a more detailed breakdown:

Term	Scope & Definition	Examples
Artificial Intelligence (AI)	**The Broad Field:** The overall science and engineering of creating intelligent machines that can perceive their environment, reason, learn, and solve problems, mimicking human intelligence.	Game-playing bots (chess), robotics on an assembly line, navigation systems (like GPS), **and** Large Language Models.
Machine Learning (ML)	**A Key Approach within AI:** A subfield of AI where systems are "trained" on large amounts of data to find patterns and make predictions or decisions *without* being explicitly programmed for that task.	Spam filters that learn to identify junk mail, recommendation engines (Netflix, Amazon), and fraud detection systems.
Large Language Model (LLM)	**A Specific Type of ML:** A highly specialized and massive machine learning model trained on vast quantities of text and code. Its specific purpose is to understand and generate human-like language. I am an example of an LLM.	Generating text, answering questions, summarizing documents, translating languages, writing code.

Border Searches

Questions

MAJ ReAnne R. Wentz

reanne.r.wentz.mil@army.mil