Digital Evidence and the Law Update

MAJ ReAnne R. Wentz
Associate Professor, The Judge Advocate General's Legal Center and School
reanne.r.wentz.mil@army.mil

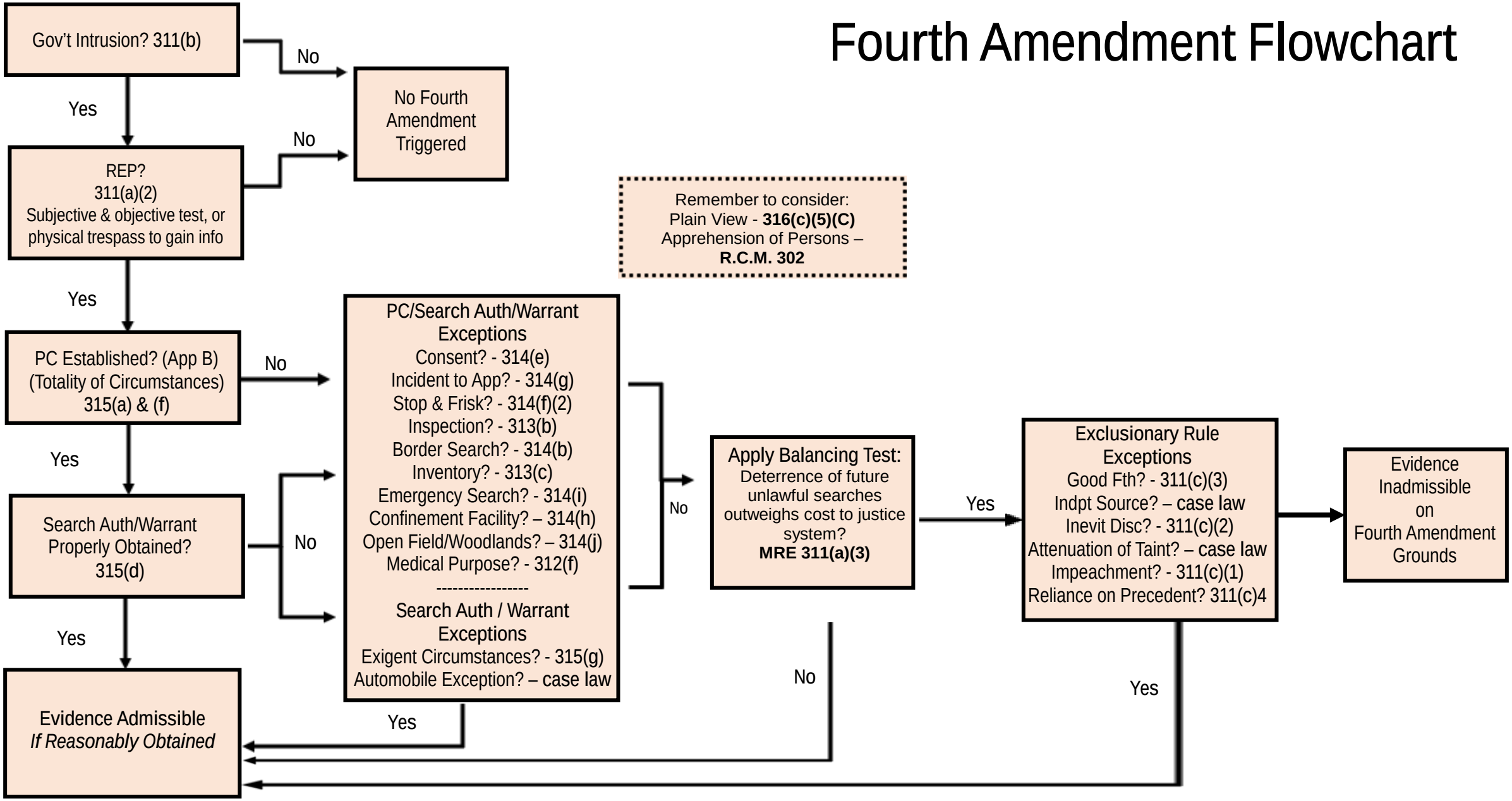
Google and Your Phone Know all Your Things

MAJ ReAnne R. Wentz
Associate Professor, The Judge Advocate General's Legal Center and School
reanne.r.wentz.mil@army.mil

Digital Evidence Affects All Areas of MJ

- Investigation (4th Amendment – private search doctrine, staleness, particularity, etc.)
- Charging (Cryptocurrency, Deepfakes. See also, *United States v. Strong*, 85 M.J. 58 (C.A.A.F. 2024))
- Discovery (See *United States v. Secord*, 2024 CCA LEXIS 263 (A. Ct. Crim. App. June 26, 2024) and *United States v. Braum*, 2024 CCA LEXIS 419 (A.F. Ct. Crim. App. Oct. 10, 2024))
- Trial (Deepfakes, AI, authentication, trial prep, professional responsibility)

Fourth Amendment Flowchart



Agenda

I. Reverse search warrants
   I. Geofencing
   II. Reverse keyword
II. Passcodes / Biometrics
III. Upcoming issues

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

Particularity

- *Andresen v. Maryland*, 427 U.S. 463 (1976)
  - "General warrants, of course, are prohibited by the Fourth Amendment. The problem posed by the general warrant is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings."
- General warrant: "whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not be granted." Constitution of Virginia, Article 1, Section 10

Particularity

- *Maryland v. Garrison*, 480 U.S. 79 (1987)
  - "The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."

Ybarra v. Illinois, 444 U.S. 85 (1979)

- Heroin in Aurora Tap Tavern in Aurora, Illinois.
- "Greg" had 25 tin-foil packets on him. LE obtained a warrant for the tavern and Greg, the heroin-dealing bartender.
- Ybarra present at the tavern and was searched. He also had heroin.
- Court held: no PC to search Ybarra, a patron. "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."

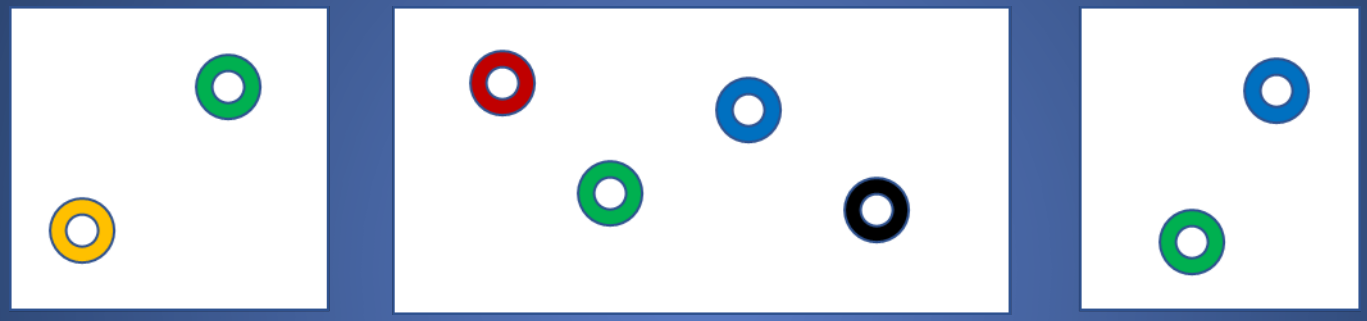
United States v. Rhine

- 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

Three step process

1. Identify all devices. This led to a total of 5,723 devices.
2. 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.
3. 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.



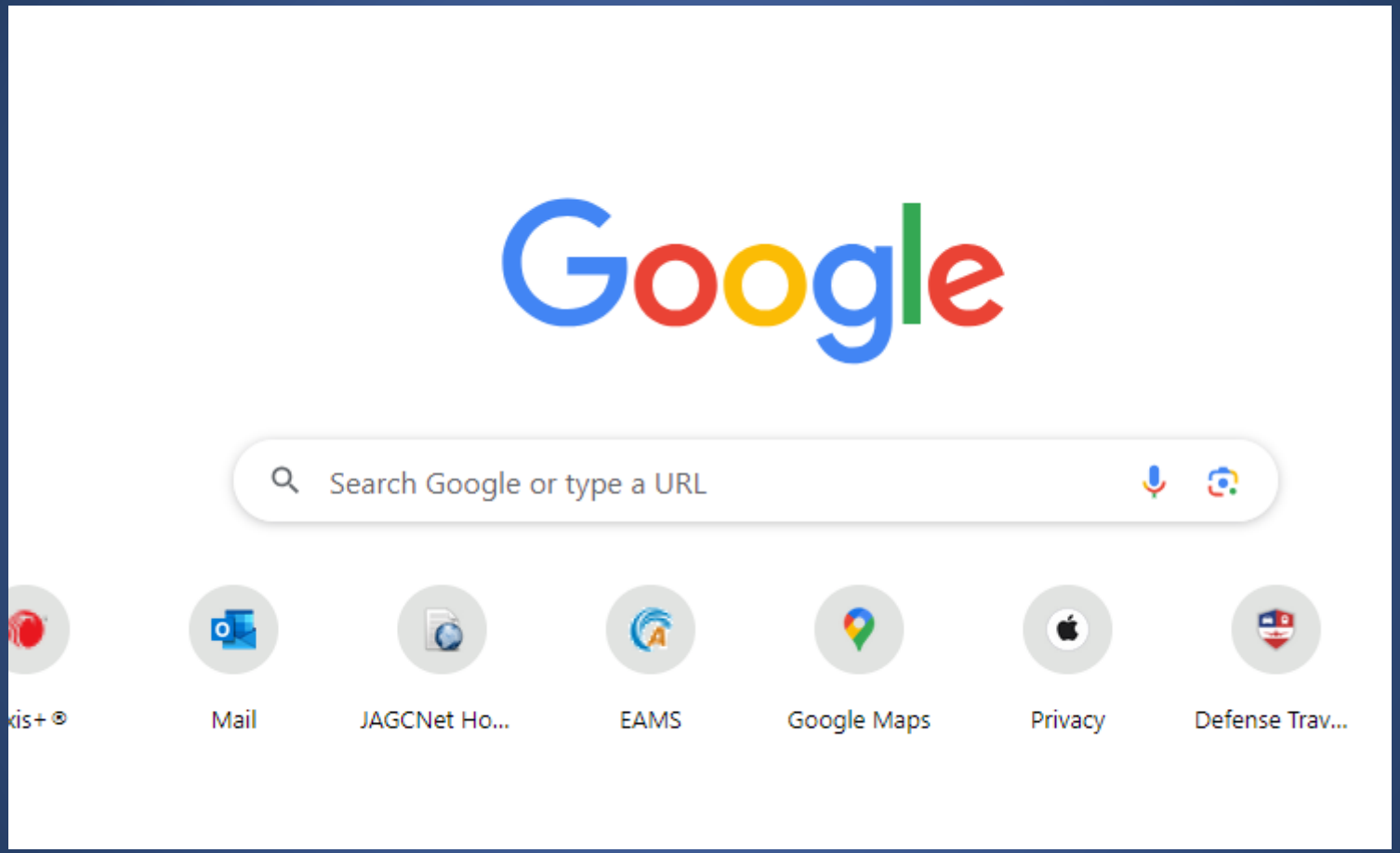
Supplemental Affidavit & Google BSI Return:

Circuit Split?

- *United States v. Chatrie* (4th Circuit)
- *United States v. Smith*, 110 F. 4th 817 (5th Cir. 2024)
  - Robbery. Geofence covered 98,192 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 in their respective data.

REVERSE KEYWORD SEARCHES

Reverse keyword searches



Browsers with Google as the default

- Chrome
- Firefox
- Safari
- Opera

What is it?

- 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.

Colorado v. Seymour, 536 P.3d 1260 (Colo. 2023)

- Court held:
  - Seymour did have a subjective and an objective expectation of privacy in his search data. Court noted that search history would shed light on an individual's religion or medical condition and other intimate details.
  - Although the Third-Party Doctrine does not allow for an objective expectation of privacy in Seymour's search data, Colorado's Constitution is more encompassing.
  - LE's copying of Seymour's Google search history meaningfully interfered with his possessory interest in his data and constituted a seizure.

Pennsylvania v. Kurtz, 294 A.3d 509 (Pa. 2023)

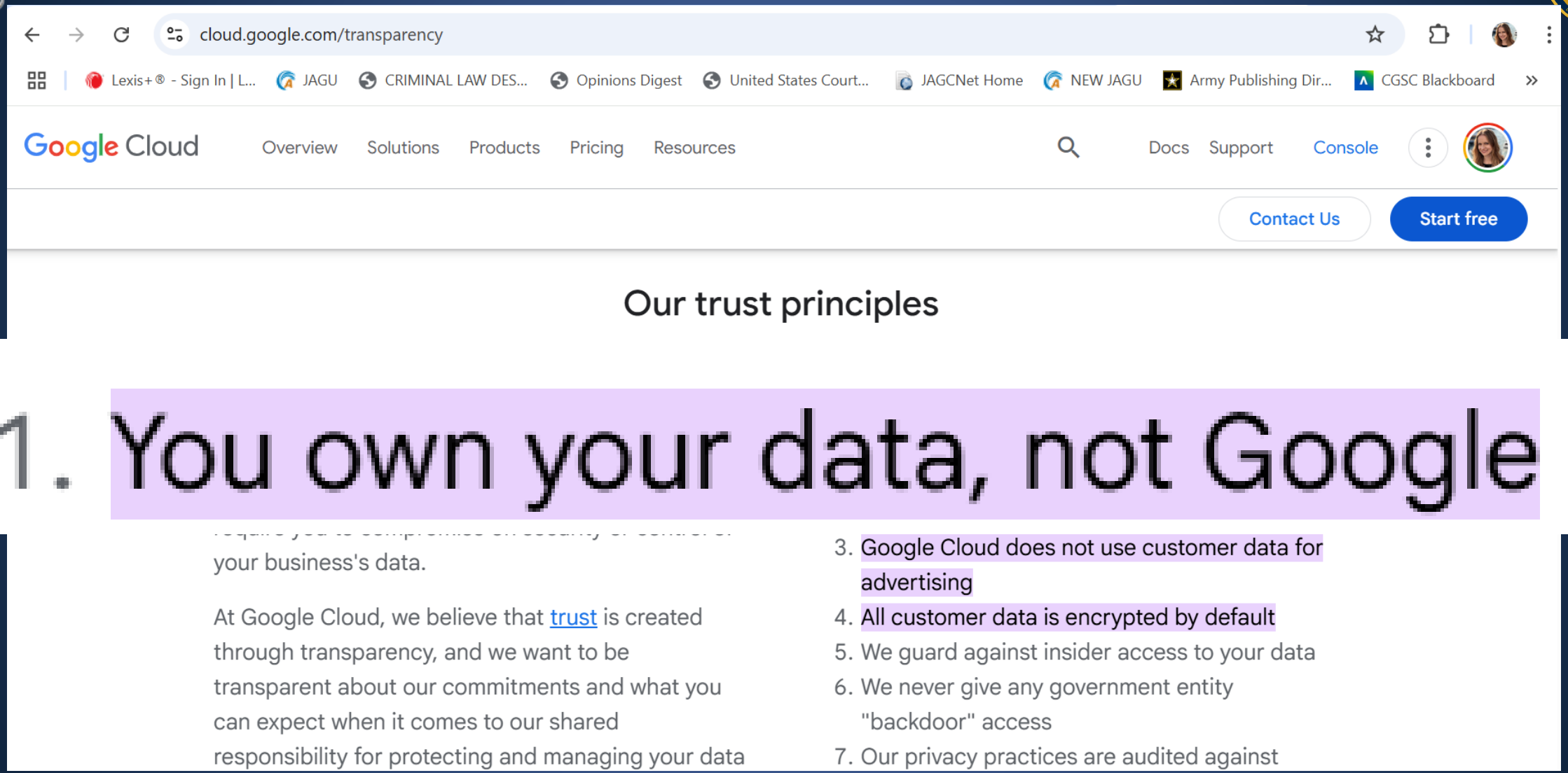
- Facts: In July, 2016, K.M. sexually assaulted in her house while her husband was working an overnight shift. Unknown assailant.
- Police obtained a search warrant directed at Google for records of searches made with Google search engine for the victim's name or home address for the week preceding the 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.

Pennsylvania v. Kurtz, 294 A.3d 509 (Pa. 2023)

- Eventually DNA connected Kurtz to the assault of K.M. and during an interview, he told LE about four other victims
- Kurtz filed a MTS of the evidence of the Google searches
- Superior Court affirmed the trial court's denial of the motion because:
  - Third party doctrine
  - Google privacy agreement
  - Warrant was supported by PC

Pennsylvania v. Kurtz, 294 A.3d 509 (Pa. 2023)

- Kurtz tried to analogize the case to *Carpenter*. Superior Court rejected the comparison:
  - Google searches are not "passively collected," but Kurtz affirmatively chose to type in the information and submit the search "notwithstanding the company's privacy policy providing that it collects and shares search queries."
  - "The information provided by Google here did not offer anything like a 'detailed chronicle' of Appellant's movements. . . The Google warrant was limited in nature, requesting only information on searches over a discrete, seven-day period for the name of one person or one physical address associated with a violent felony. . . the warrant did not require production of data that shed light on Appellant's political views, health information, or other sensitive matters."


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

PASSCODES

Potential issues

- What is testimonial and communicative?
- Physical trait / immutable characteristics
- Privacy?
- Foregone conclusion doctrine
- Act of production doctrine

Testimonial

- "In order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a witness against himself."
  - *Doe v. United States*, 487 U.S. 201 (1988)

What about privacy?

- “But the Court has never suggested that every invasion of privacy violates the privilege. Within the limits imposed by the language of the Fifth Amendment, which we necessarily observe, the privilege truly serves privacy interests; but the Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which, in the Court's view, did not involve compelled testimonial self-incrimination of some sort
  - *Fisher v. United States*, 425 U.S. 391 (1976)

Foregone conclusion?

- "The Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production – such as the existence, custody, and authenticity of evidence – is a foregone conclusion that adds little or nothing to the sum total of the Government's information."
  - *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017) (citing *Fisher*)

Act of production doctrine

- “The act-of-production doctrine recognizes that physical acts can be ‘communicative’ ‘wholly aside from the contents’ of anything produced. . . when the action "impl[ies] assertions of fact. . . .”
  - *United States v. Brown*, 125 F.4th 1186, 1203 (5th Cir. 2025)

Mitchell, Robinson and *Nelson*

Mitchell – Accused invoked his right to counsel. LE obtained a search authorization. CAAF held that asking for Mitchell's pin was a violation of his 5th Amendment rights.

Robinson – Accused invoked his right to counsel. LE asked for consent to search his phone and the passcode. CAAF held that it was NOT a violation of his 5th Amendment rights.

Nelson – Accused waived and then said he wanted a lawyer to look at texts. LE obtained a search authorization and asked for the passcode. CAAF held that it was not a violation of his 5th Amendment rights.

BIOMETRICS

United States v. Payne, 99 F.4th 495 (9th Cir. 2024)

- Police pulled over appellant and forced his thumb on his phone to open it.
- For 5A purposes, physical traits are not testimonial. The actions of the police "do not involve the testimonial capacities of the accused and instead only compel an individual to provide law enforcement with access to an immutable physical characteristic."
- SCOTUS "has framed the question around whether a particular action requires a defendant to divulge the contents of his mind, not whether two actions yield the same result."

United States v. Brown, 125 F.4th 1186 (5th Cir. 2025)

- Police obtained Schwartz's thumbprint to open the phone.
- "[T]he compelled opening of a cell phone itself directly announces the owner's access to and control over the phone, as well as his mental knowledge of how to unlock the device. There is no additional information that is needed . . . forcing Schwartz to open the phone was testimonial."
- Physical trait and act of production doctrines

United States v. Gilkey

- 2025 CCA LEXIS 86 (A. Ct. Crim. App. March 4, 2025)
- Court held:
  - CID was required to advise Gilkey of his rights
  - CID interrogated Gilkey when they were asking him questions about his defense counsel's phone number. His "response not only gave the government access to direct evidence, but also 'constituted direct evidence.'"
  - Adopts the reasoning in *U.S. v. Brown*

What's Next?

- How to navigate authentication in a world of AI
- How to charge deepfake nonconsensual distribution of intimate images
- How to charge AI-generated child sexual abuse material
- How to navigate use of records held by data brokers

Questions?

MAJ ReAnne R. Wentz

reanne.r.wentz.mil@army.mil