Digital Evidence and the Law Update
Major ReAnne Wentz
Court of Appeals for the Armed Forces CLE
May 2026

I. Intro –
   i. Too much in too little time.
   ii. Agenda: Geofencing, Reverse Keyword Searches, AI, Border Searches
   iii. The increased amount of data that we are all making and leaving is being used by law enforcement

II. Geofencing
   a. What is geofencing?
   b. Is it still viable now that Google is out of the game?
   c. What is a geofence warrant? A multi-step search warrant that seeks the user information for anyone who was within a certain geographical area during a certain time.
      i. *United States v. Rhine*, 652 F. Supp. 3d 38 (D.D.C. 2023)
      ii. Three-step process
   d. Concerns with geofencing warrant
      i. Particularity
         1. *Marron v. United States*, 275 U.S. 192 (1927)
         2. *Andresen v. Maryland*, 427 U.S. 463 (1976)
            a. "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."
         3. *Maryland v. Garrison*, 480 U.S. 79 (1987)
            a. "The manifest purpose of the particularity requirement was to prevent general searches."
         4. *Ybarra v. Illinois*, 444 U.S. 85 (1979)
            a. "Each patron who walked into the Aurora Tap Tavern on March 1, 1976, was clothed with unconstitutional protection against an unreasonable search or an unreasonable seizure."
   e. Circuit split:
      i. *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2023) (rehearing en banc granted *United States v. Chatrie*, 2024 U.S. App. LEXIS 27770 (4th Cir. November 1, 2024)).
         1. Third-Party Doctrine applied and therefore, Chatrie had no reasonable expectation of privacy in his Google location history and the procurement of that data was not in violation of the Fourth Amendment
         2. SCOTUS granted certiorari, with oral argument scheduled for 27 April 2026. All filings here: https://www.scotusblog.com/cases/case-files/chatrie-v-united-states/
      ii. *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024)
         1. The Third-Party Doctrine does not apply, the two appellants had a reasonable expectation of privacy in their respective data and the third-party doctrine does not apply.

III. Reverse keyword searches
   a. What are reverse keyword searches? Multi-step search warrants that request the user information for anyone who searched for certain information – typically, addresses.
   b. CrimPro Refresher
      i. *Katz v. United States*, 389 U.S. 347 (1967)
      ii. *Smith v. Maryland*, 442 U.S. 735 (1979)
      iii. Post-*Carpenter v. United States*, 585 U.S. 296 (2018)
         1. Mosaic Theory
         2. Factors SCOTUS considered: intimacy, comprehensiveness, expense, retrospectivity, and voluntariness
   c. *Colorado v. Seymour*, 536 P.3d 1260 (Colo. 2023)
      i. Appellant had a subjective and objective expectation of privacy in his data
      ii. Third-Party Doctrine applied, but Colorado constitution provided a "constitutionally protected privacy interest in his Google search history."
      iii. Good Faith Exception applied
   d. *Pennsylvania v. Kurtz*, 348 A.3d 133 (Pa. 2025)
      i. There is no reasonable expectation of privacy in internet searches because the information is voluntarily shared with e.g., Google.
      ii. BL: Google searches fall within the traditional third-party doctrine.
   e. Google isn't the only game in town and ChatGPT is obtaining must more personal data
      i. Bridget Reineking, *Chatbot, Can You Keep a Secret? Protecting Warrantless Searches of Algorithm Prompts in the Age of AI*, 38 Regent U.L.Rev. 90 (2026)
      ii. 56% of people in a survey had "asked chatbots for legal advice." In the same study, "50% of AI users were unaware that their ChatGPT conversations could be subpoenaed." Which makes the question about the Reasonable Expectation of Privacy test a complicated one. See, *Katz v. United States*, 389 U.S. 347 (1967)
         1. https://www.kolmogorovlaw.com/the-chatgpt-subpoena-revolution-when-your-ai-conversations-become-court-evidence.
      iii. ChatGPT is helping people commit crimes. e.g. AI-generated CSAM.

IV. AI
   a. What is it?
      i. Artificial Intelligence: "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."
      ii. Machine Learning: "a subfield of AI where systems are 'trained' on large amounts of data to find patterns and make predictions or decisions without being explicitly programed for that task"
      iii. Large Language Model: "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."
      iv. Source: Gemini Enterprise, GenAI.mil

b. AI can "hallucinate": https://hai.stanford.edu/news/ai-trial-legal-models-hallucinate-1-out-6-or-more-benchmarking-queries

V. Border Searches

a. M.R.E. 314(b)
    i. "Evidence from a border search for customs or immigration purposes authorized by a federal statute is admissible."
b. Another CrimPro Review:
    i. *Riley v. California*, 573 U.S. 373 (2014)
        1. LE need a warrant to search a cell phone incident to arrest
    ii. Searches not for the purpose of obtaining evidence
        1. Inventories
        2. Incident to arrest
    iii. *United States v. Ramsey*, 431 U.S. 606, 616 (1977)
        1. "[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virgue of the fact that they occur at the border . . ."
    iv. "[B]order searches have long been exempted from warrant and probable cause requirements, and ordinarily are reasonable simply by virtue of the fact that they occur at the border."
        1. *United States v. Mendez*, 103 F.4th 1303, 1307 (7th Cir. 2024)
c. *United States v. Ramos*, 659 F.Supp.3d 779, 798 (W.D. Tex. 2023)
    i. "As noted, warrantless, nonconsensual searches 'are per se unreasonable' under the Fourth Amendment 'unless they fall within a few narrowly defined exceptions,' such as the border search exception . . . . Whether—and under what circumstances—the border search exception empowers the Government to forensically search electronic devices without a warrant 'is an area of evolving jurisprudence" that has divided federal courts.'"
d. *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019)
e. *United States v. Castillo*, 70 F.4th 894, 898 (5th Cir. 2019)
    i. "No reasonable suspicion is necessary to conduct the sort of routine manual cell phone search at the border that occurred here."
f. *United States v. Quarles*, 2025 U.S. App. LEXIS 12086 (11th Cir. 2025)
g. *United States v. Nkongho*, 107 F.4th 373 (4th Cir. 2024)
h. Jacob Pagano, *Smart Phones at the Border: What Does the Fourth Amendment Protect?*, Lawfare, September 20, 2023. https://www.lawfaremedia.org/article/smart-phones-at-the-border-what-does-the-fourth-amendment-protect
i. *Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment*, Congressional Research Service, Number LSB10387, March 17, 2021. https://www.lawfaremedia.org/article/smart-phones-at-the-border-what-does-the-fourth-amendment-protect.
j. Note: *The Border Search Muddle*, 132 Harv. L. Rev. 2308 (2019) https://harvardlawreview.org/print/vol-132/the-border-search-muddle/#footnotes-container

VI. Searching cell phones, generally
   a. Mil. R. Evid. 304(b) – derivative evidence
   b. Passcode issue – Fifth Amendment problem, rather than Fourth Amendment
   c. Military caselaw relating to passcodes
      i. *United States v. Mitchell*, 76 M.J. 413 (C.A.A.F. 2017)
      ii. *United States v. Robinson*, 77 M.J. 303 (C.A.A.F. 2018)
      iii. *United States v. Nelson*, 82 M.J. 251 (C.A.A.F. 2022)
   d. Biometrics
      i. *United States v. Payne*, 99 F.4th 495 (9th Cir. 2024)
      ii. *United States v. Brown*, 125 F.4th 1186 (D.C. Cir 2025)