



4TH & 5TH AMENDMENT ISSUES WITH DIGITAL EVIDENCE IN CRIMINAL JUSTICE



Continuing Legal
Education

Direct
Assistance



Special Victim
Prosecutors

MAJ Heather Tregle
Chief, Complex Litigation
Trial Counsel Assistance Program

“[C]ell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society.”

Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (citations and internal quotations omitted)



CELL PHONE PASSCODES



United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017)

- Invoked Article 31b rights to silence and counsel
- 2 hours later, ordered to the commander's office
- CID agent had a valid search authorization to seize and search phone
- Accused refused to provide passcode when asked "can you give us PIN"
- "if you could unlock it, great, if you could help us out. But if you don't, we'll wait for a digital forensic expert to unlock it."
- Accused then permanently disabled the passcode on his phone.



United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017)

HELD:

- 1) Custodial interrogation, both at CID and CO's office
- 2) Violation of 5th Amendment under *Miranda* and *Edwards*
- 3) Asking accused to enter it himself rather than tell them the passcode still constituted interrogation (citing to, inter alia, *United States v. Hubbell*, 530 U.S. 27, 29 (2000) ("contents of his own mind")).



United States v. Robinson, 77 M.J. 303 (C.A.A.F. 2018)

Seven months later...

- Accused invoked right to counsel
- AFOSI asked if they could search accused's cell phone
- Accused gave verbal & written consent, knowing it was to look for evidence of the crime about which he'd just been advised
- AFOSI asked for, and received, the passcode
- AFOSI took the phone, entered the passcode, forensically imaged the entire phone, gave it back.

HELD:

No *Edwards* violation



What's different?

“[W]hen the investigator asked Appellant for consent to search his cell phone, that inquiry fit squarely within the consent to search exception of *Edwards*...Moreover, we conclude that when the investigator shortly thereafter asked Appellant for the passcode to that cell phone for the sole purpose of effectuating the search that he had just voluntarily consented to, that second inquiry was merely a natural and logical extension of the first permissible inquiry. Thus, because of its nature, purpose, and scope, this second inquiry similarly did not rise to the level of a reinitiation of interrogation.” *Robinson*, 77 M.J. at 306.

“[B]adgering an unrepresented suspect into granting access to incriminating information threatens the core Fifth Amendment privilege, even if the government already knows that the suspect knows his own password.” *Mitchell*, 76 M.J. at 419.



United States v. Nelson, 85 M.J. 251 (2022)

Most recently...

- Custodial interrogation, advised, waived rights.
- During interrogation, asked 5 times for consent to search cell phone. Declined.
- Investigator seized phone and terminated the interview.
- Investigator obtained search authorization for the contents of the phone.
- One day after previous interrogation, without re-advising of rights, investigator informed Accused he had a search authorization, and put the phone in front of him.
- Asked if he was willing to unlock his cell phone.
- Responded: “I guess I don’t have a choice.”
- Without waiting for a response, he immediately unlocked his phone.

HELD: “We conclude that under the ‘totality of the circumstances’ there is not a basis for us to conclude the Appellant’s entry of his passcode was involuntary.”



A loophole!






United States v. Hunt, 2019 CCA Lexis 310 (A.F. Ct. Crim. App., Jul. 11, 2019)



Consistent with AFOSI's practice for cell phones at the time, the military magistrate also ordered Appellant to unlock the cell phone via passcode or biometrics. When Appellant was presented with the military magistrate's order, he unlocked his phone. Appellant did not consent to unlock his phone and only did so after reviewing the order. SA PM could not recall whether Appellant unlocked the phone via passcode or biometrics. SA PM seized the phone once Appellant unlocked it.



Does that matter?

Results for: cell phone biometric   

Must include: "biometric" "cell phone" [Clear](#)

Cases	551	Military Justice  Clear 
Statutes and Legislation	10,000+	
Practical Guidance	434	
Secondary Materials	10,000+	

No documents found in Cases filtered by Military Justice.

...probably...

Where, as here, the Government agents will pick the fingers to be pressed on the Touch ID sensor, there is no need to engage the thought process of the subject at all in effectuating the seizure. The application of the fingerprint to sensor is simply the seizure of a physical characteristic, and the fingerprint by itself does not communicate anything. It is less intrusive than a forced blood draw. Both can be done while the individual sleeps or is unconscious. Accordingly, the Court determines—***in accordance with a majority of Courts that have weighed in on this issue***—that the requested warrant would not violate the Fifth Amendment because it does not require the suspect to provide any testimonial evidence.

In re search of A White Google 3 XI Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793-94 (D. Idaho 2019)(emphasis)



But, also consider.

“We also share the concerns voiced by other courts that holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance. The distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context.”

State v. Andrews, 243 N.J. 447, 480 (2020).

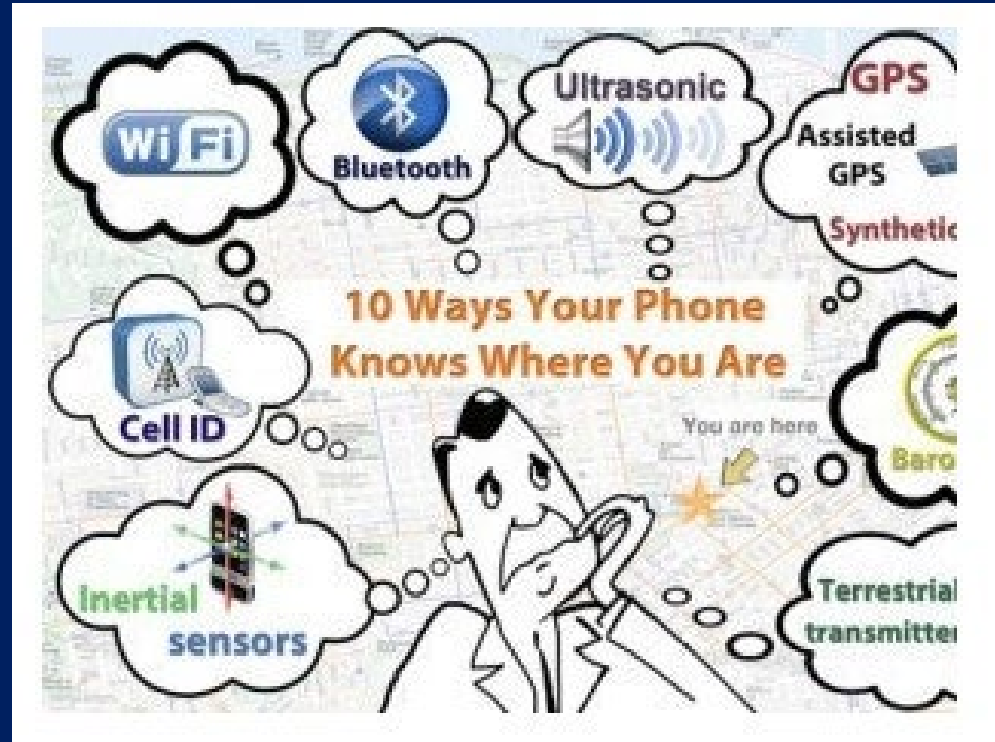


Other Cases Related to Passcodes

- *United States v. Painter*, 2020 CCA Lexis 474 (A.F. Ct. Crim. App., Dec. 23, 2020) (inevitable discovery based on DFE's ability to break passcode encryption)
- *United States v. Black*, 2022 CCA Lexis 614 (C.A.A.F., Aug. 25, 2022) (third party consent doctrine)
- *United States v. Drinkert*, 81 M.J. 540 (N-M.C. Ct. Crim. App. 2021) (application of *Wallace* factors and "officer safety" exception to seizure and search of phone)
- *United States v. Booker*, 2021 U.S. Dist. Lexis 177641 (S.D. Cal., Sept. 17, 2021) (granting suppression after NCIS agent compelled passcode)



GEOLOCATION DATA



Any opportunity for privacy?

TECH

Google Opt Out Feature Lets Users Protect Privacy By Moving To Remote Village

| 8/11/09 8:07AM

Web users who choose to move to the desolate village are guaranteed an environment free from Google products and natural light from the sun.



Carpenter v. United States, 138 S.Ct. 2206 (2018)

Cell Site Location Information (CSLI), even though collected privately by a third party as an incident to using a cell phone, cannot be searched without a warrant

Declined to extend the *Miller* third party consent doctrine to CSLI

BUT...

Our decision today is a narrow one. We do not ... address other business records that might incidentally reveal location information.

138 S. Ct. at 2220



So what about?

ZIP code

Password – minimum 6 characters

Sign Up

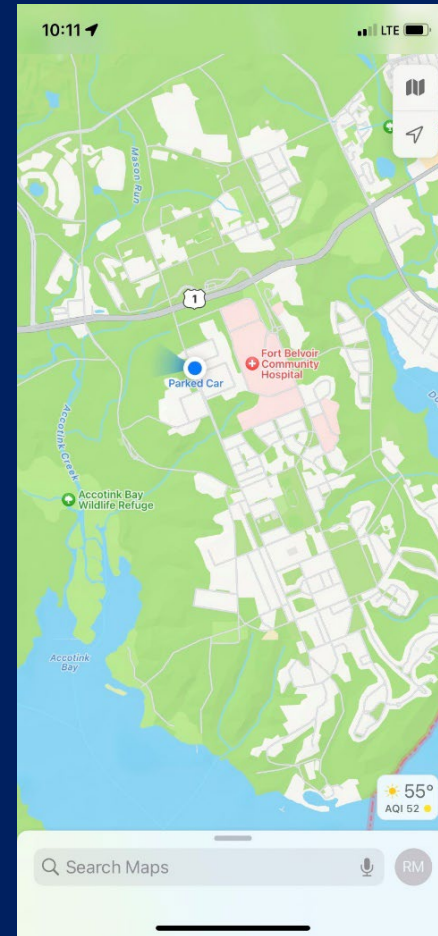
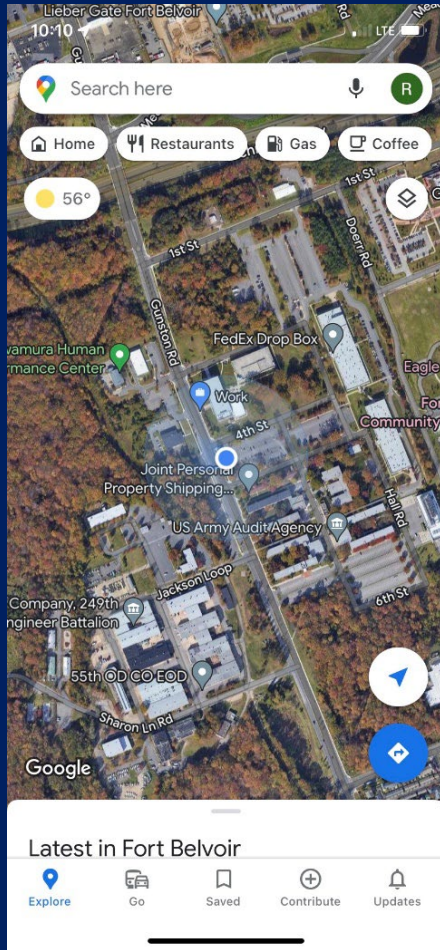
By clicking Sign Up, you agree to our Terms of Service and that you have read our Privacy Policy.

Carpenter held not to apply to...

- Public Cameras. *United States v. Trice*, 2020 U.S. App. Lexis 22738 (6th Cir. 2020)
- GPS Ankle Monitors. *United States v. Lambus*, 897 F.3d. 368 (2d. Cir 2018)
- “Real-time CSLI” [vice stored “historical” CSLI]. *United States v. Hargett*, 797 Fed. Appx. 765 (4th. Cir. 2020)
- IP Addresses. *United States v. Hood*, 920 F. 3d 87 (1st Cir. 2019)
- Cryptocurrency account logs. *United States v. Gratkowski*, 2020 U.S. App. Lexis



What's left?



Compare

United States v. Diggs, 358 F. Supp. 3d 648 (N.D. Ill. 2019)

- Lexus car dealer installed GPS on some vehicles; drivers consented to allowing Lexus using it “to find the vehicle
- Police asked Lexus to find a suspect’s car for them; Lexus employee used own account/access]

HELD:

1)The GPS data at issue here fits squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*.

2)Applying the third-party doctrine to the GPS data here would require essentially the same extension of the doctrine that the Court rejected in *Carpenter*.

In re Google Location History Litigation, 428 F. Supp. 3d. 185 (N.D. Cal. 2019)

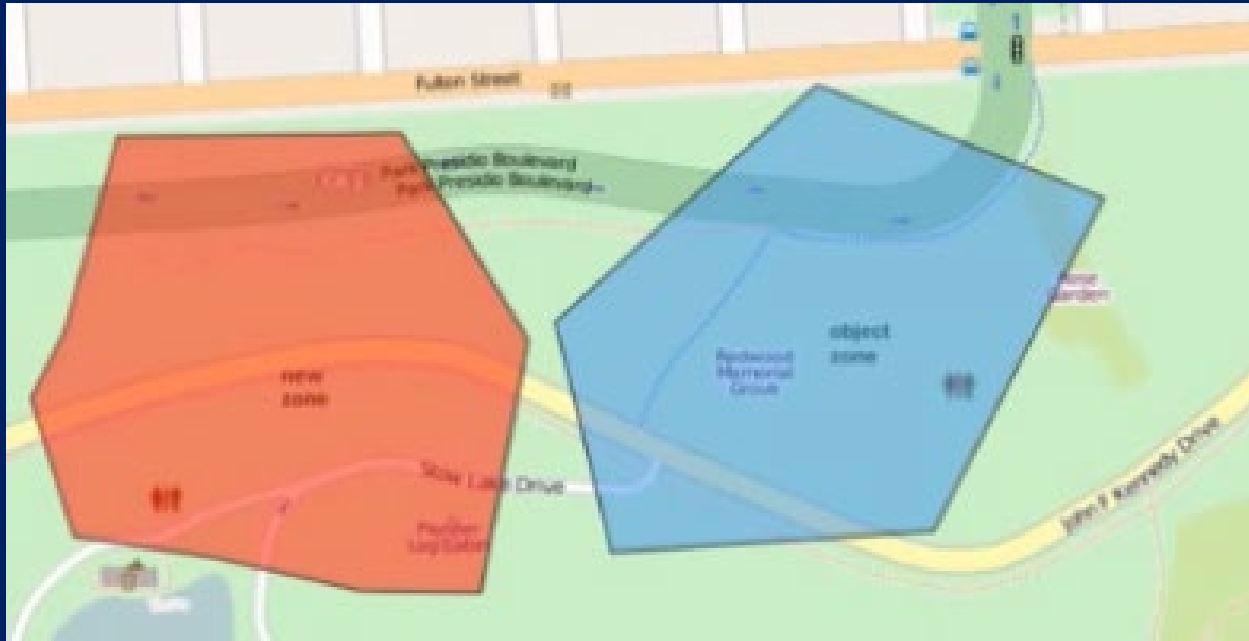
- Argued that, even with location history turned off, Google was still tracking users’ locations and storing it [tort action]
- “consent to geolocation tracking is corollary to the use of a Google service, like Google Maps.”

HELD:

- 1) Defendant’s “profile” of a user is only as specific as their use of Google services. *Carpenter v. United States* and *United States v. Jones* do not undercut this conclusion.
- 2) The cell-site location information discussed in *Carpenter* was comprehensive...Such comprehensive data collection is not at issue here; Plaintiffs’ geolocation information depends on how often they use Google’s services. Defendant’s collection of geolocation data is not automatic; it does not happen by the routine “pinging” of a cell-tower.



GEOFENCES



Google received its first [geofence warrant] in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate . . . increased over 500% from 2018 to 2019." In 2019,

Google received "around 9,000 total geofence requests."

And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States.

United States v. Chatrue, No. 3:19cr130, 2022 U.S. Dist. LEXIS 38227, at *23 (E.D. Va. Mar. 3, 2022)



Results for: geofence

<input type="checkbox"/> Federal	42
+ <input type="checkbox"/> 2nd Circuit	1
+ <input type="checkbox"/> 3rd Circuit	4
+ <input type="checkbox"/> 4th Circuit	5
+ <input type="checkbox"/> 5th Circuit	6
+ <input type="checkbox"/> 6th Circuit	4
+ <input type="checkbox"/> 7th Circuit	4
+ <input type="checkbox"/> 8th Circuit	1
+ <input type="checkbox"/> 9th Circuit	6
+ <input type="checkbox"/> 10th Circuit	3
+ <input type="checkbox"/> 11th Circuit	7
+ <input type="checkbox"/> D.C. Circuit	1

What information is out there?

“Location History is powerful: it has the potential to draw from **Global Positioning System ("GPS") information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ("IP") address information, and the signal strength of nearby Wi-Fi networks.** According to Agent [D], Location History logs a device's location, **on average, every two minutes.** Indeed, Location History even allows Google to "estimat[e] where a device is in terms of elevation.”

“Google stores this data in a repository known as the "Sensorvault" and associates each data point with a unique user account. The Sensorvault contains a substantial amount of information. [M] testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and **receives and stores all location history data in the Sensorvault** to be used in ads marketing.”

“Once a user opts into Location History, Google is ‘**always collecting**’ data and storing *all* of that data in its vast Sensorvault, even ‘if the person is not doing anything at all with [his or her] phone.’”

Chatrie, 2022 U.S. Dist. LEXIS 38227, at *7-10 (Emphasis added)



How does Google respond to a Geofence warrant?

- 1) A warrant compelling a “de-identified” list of all users whose location history data indicates their devices were within the geofence, as defined by both time and space. Google produces the responsive records identified in Sensorvault, including an anonymized “device number” and the lat/long coordinates and timestamp, as well as the source (GPS, Wi-Fi, cell tower, etc.)
- 2) Government must review the de-identified data to determine the devices of interest. (E.g., devices not in the area long enough, transiting through the area, or their movements were inconsistent with other evidence in the case. Google’s internal policy typically requires the government to narrow it to *some* degree. Government can then request additional location data for those devices *outside* the time and space of the geofence.
- 3) After receiving the response to the Step 2 request, the Government can then compel production of account-identifying information. “Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is possible that Google would approve a Step 3 request that is not narrowed after Step 2 at all.”

Chatrie, 2022 U.S. Dist. Lexis 38277 at *24-29.



The 4th 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.

...particularly describing the place to be searched...

[E]nsures 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.

Maryland v. Garrison, 480 U.S. 79 (1987)



Same district court, 2 different results:

In re Search of Information Stored at Premises Controlled by Google, 481 F. Supp. 3d 730 (N.D. Ill. 2020)

- Clear PC that a crime occurred at the time/place to be searched, and a “fair probability” that Google had evidence related to the crimes in its possession
- Rejected the argument that the 3-step process protected privacy of the innocent, since the warrant would only be required at Step 1.
- “There is likely a fair probability that the Amended Application's proposed warrant will generate location information, and device IDs that are the functional equivalent of the identities of the device users, that will *include* the identification of the Unknown Subject and will thus *include* evidence of the crime, but it will include other information as well: The location information of persons not involved in the crime.”



Same district court, 2 different results:

In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020)

- “Ample” PC to establish crime of arson at the time/place
- Noted the ubiquity of cell phones, c.f. *Carpenter*, and the reasonable inference that criminals coordinating multiple arsons would have cell phones on them
 - Government “has structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses.” 15-30 minute windows
 - Target locations principally limited to the property of the victim business
 - Warrant limited in scope, affiant agent provided specific items of evidence already uncovered in the investigation to narrow down the possible leads/suspects
- “The government's affidavit must provide sufficient information on how and why cell phones may contain evidence of the crime, as well as credible information based on the agent's training and experience, to support the assertions.”



Common Concerns

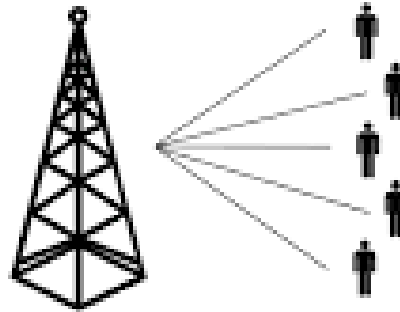
- Nexus between crime or suspects and devices
- PC to believe that evidence of the crime will be found in the time/place searched
- Particularity to avoid overbreadth and infringing on the privacy of uninvolved individuals
- “It is also important to recognize that the Fourth Amendment does not deal in precision, but rather probability.”



Taking out the middle man...



REGULAR CELL PHONE COMMUNICATIONS



COMMUNICATIONS WITH A CELL SITE SIMULATOR



QUESTIONS?



Trial Counsel Assistance Program
9275 Gunston Road
Fort Belvoir, Virginia 22060-5546

Your briefer today:

MAJ Heather L. Tregle

Heather.l.tregle.mil@army.mil

571-234-3849



TCAP E-mail: usarmy.pentagon.hqda-otjag.list.usalsa-tcap

COL Robert Stelle, Chief

LTC Stacey Cohen, Deputy Chief

CW2 Terrence Jenkins, Legal Administrator

SFC Justin Rey-Taft, SVPNCO PM

Eleanor Odom, Special Victim Litigation Expert

Bridget Ryan, Special Victim Litigation Expert

Kathryn Marsh, Special Victim Litigation Expert

MAJ Heather Tregle, Chief, Complex Litigation

MAJ Andrew Ground, Complex Litigation Team

CPT Erin Kiss, Training Officer

CPT Eli Ross, Training Officer

CPT Matthew Bishop, Training Officer

