



---

**PROGRAM MATERIALS**

**Program #36158**

**May 11, 2026**

# **Electronic Information in Criminal Investigations & Prosecutions: Constitutional and Admissibility Issues**

**Copyright ©2026 by**

- **Ron Hedges, Esq. - Ronald J. Hedges LLC**

**All Rights Reserved.  
Licensed to Celesq®, Inc.**

---

**Celesq® AttorneysEd Center**  
**[www.celesq.com](http://www.celesq.com)**

**5301 North Federal Highway, Suite 150, Boca Raton, FL 33487**  
**Phone 561-241-1919**

# **ELECTRONIC INFORMATION IN CRIMINAL INVESTIGATIONS & PROSECUTIONS: CONSTITUTIONAL AND ADMISSIBILITY ISSUES**

Celesq AttorneysED Center

MAY 11, 2026

11:00 – NOON ET

# PRESENTER

## RONALD J. HEDGES

- Principal, Ronald J. Hedges LLC
- United States Magistrate Judge, District of New Jersey, 1986-2007
- Co-Senior Editor, *Sedona Conference Cooperation Proclamation: Resources for the Judiciary Fourth Edition* (August 2025) and prior versions
- Lead Author, *Managing Discovery of Electronic Information, Third Edition* (Federal Judicial Center: 2017)
- Chair of Court Technology Committee of ABA Judicial Division
- Member, NJSBA Artificial Intelligence Committee
- Member, NYSBA AI & Emerging Technologies Committee
- Contact at [r\\_hedges@live.com](mailto:r_hedges@live.com)

# DISCLAIMER

- The information in these slides and presentations is not legal advice and should not be considered legal advice.
- This presentation represents the personal views of the presenters.
- This presentation is offered for informational and educational uses only.

# AGENDA

1. Introduction to Electronic Information in Criminal Matters
2. Applicability of Fourth Amendment to electronic information sought or secured by law enforcement
3. Applicability of Fifth Amendment to electronic information sought or secured by law enforcement
4. Applicability of the Sixth Amendment right of confrontation
5. Admissibility

# INTRODUCTION

## *UNITED STATES v. MALINDRETOS*

- Charged with attempted use of fire to damage and destroy a building within the District of New Jersey
- Tracked by:
  - Surveillance video at building
  - License plate reading device (“LPR”)
  - Video cameras in the area where suspect’s car was parked

# INTRODUCTION

## *I/M/O APP. FOR SEARCH WARRANT*

- Multiple murders in Idaho, search warrant issued for suspect's residence in Washington State
- Supporting declaration included these sources of electronic information:
  - Video footage from bar
  - Livestreamed video from food truck
  - Downloads of records from victims' phones
  - Security camera at scene of crime
  - Video canvass of surveillance videos in neighborhood
  - Law enforcement body camera
  - License plate reader
  - Open-source internet search
  - Historical CSLI

# INTRODUCTION

## *I/M/O APP. FOR SEARCH WARRANT*

- Warrant sought, among other things:
  - “images, whether digital or on paper ”
  - “Trace evidence including DNA”
  - “Data compilations (whether digital/electronic or on paper or other format)”
  - “Electronic/digital devices or digital storage devices”
  - “Evidence of other accounts associated with this device”
  - “related data created, accessed, read \*\*\* between the above dates”
  - “Evidence of use of the device to conduct internet searches”
  - “Information that can be used to calculate the position of the device”
  - “Evidence of the identity of the person in possession of the device”

# INTRODUCTION

## THE LAS VEGAS CYBERTRUCK

Prompts to ChatGPT:

- “How much Tannerite is equivalent to 1 pound of TNT?’ He follows up by asking how it might be ignited at ‘point blank range.’”

See D. Cameron, “Before Las Vegas, Intel Analysts Warned that Bomb Makers were Turning to AI,” *Wired* (Jan. 8, 2025)

# INTRODUCTION

## THE JUDGE AND THE VR HEADSET

See “Judge Wears VR Headset To View Defendant's Account Of Events And What Fresh Hell Is This?” *Above the Law* (Jan. 9, 2025)

- Who supports the tech?
- Who pays for it?
  - Court?
  - Defendant?
    - Retained counsel?
    - Public defender?
  - Prosecution?
  - Is the use of VR a case of “buying justice?”
- What is the appellate record?

# INTRODUCTION

## KNOWN OR FORESEEABLE

Criminal Causes of action arising out of GAI include:

- Child pornography
  - *United States v. Morton*, 950 F.3d 257 (5<sup>th</sup> Cir. 2020)
- Data breach
- Cybersecurity
- Malicious use, such as deep fakes, hate speech and scamming
- And what else?

# FOURTH AMENDMENT\*

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

- Microphones on telephone booths
- Wires leading to wire recorders
- Search warrant for bookmaking records, etc.

How have times changed?

\*But note that the State constitutions may offer greater protection to New Jersey residents than the Fourth Amendment. See, e.g., *State v. Earls*, 214 N.J. 564 (2013).

# FOURTH AMENDMENT

*United States v. Jones*, 565 U.S. 400 (2012):

- Scalia (with Roberts, Kennedy and Thomas) = “trespass”
- Alito (with Ginsburg, Breyer and Kagan) = “The best that we can do \*\*\* is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have been anticipated.” 565 U.S. at 430.
- Sotomayor = Joins Scalia’s opinion but notes that “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” 565 U.S. at 417.

# FOURTH AMENDMENT

*Riley v. California*, 573 U.S. 373 (2014):

- Unanimous decision by Roberts, C.J.
- “Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different.”
- “Our answer to the question of what police must do before searching a cell phone incident to an arrest is accordingly simple – get a warrant.”
- “Exigent circumstances” remain available.

# FOURTH AMENDMENT

*Carpenter v. United States*, 585 U.S. 296 (2018):

- Roberts, C.J. (with Ginsburg, Breyer, Sotomayor and Kagan) = acquisition of CSLI was a “search”
- Kennedy (with Thomas and Alito) = “This case involves new technology, but the Court’s stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.”

# FOURTH AMENDMENT AND GEOFENCING

- *United States v. Chatrie*, 136 F.4th 100 (4<sup>th</sup> Cir. 2025)
- *United States v. Davis*, 109 F.4th 1320 (11<sup>th</sup> Cir. 2024)
- *United States v. Smith*, 110 F.4th 817 (5<sup>th</sup> Cir. 2024)

# FOURTH AMENDMENT AND GEOFENCING

*United States v. Chatrue*, cert. granted, No. 25-112, 2026 WL 120676  
(Jan. 16, 2026)

“QUESTION PRESENTED:

This case concerns the constitutionality of geofence warrants. For cell phone users to use certain services, their cell phones must continuously transmit their exact locations to their service providers. A geofence warrant allows law enforcement to obtain, from the service provider, the identities of users who were in the vicinity of a particular location at a particular time.

(continued on next slide)

# FOURTH AMENDMENT AND GEOFENCING

In this case, law enforcement obtained, and served on Google, a geofence warrant seeking anonymized location data for every device within 150 meters of the location of a bank robbery within one hour of the robbery. After Google returned an initial list, law enforcement sought - without seeking an additional warrant - information about the movements of certain devices for a longer, two-hour period, and Google complied with that request as well. Then - again without seeking an additional warrant-law enforcement requested de-anonymized subscriber information for three devices. One of those devices belonged to petitioner Okello Chatrie. Based on the evidence derived from the geofence warrant, petitioner was convicted of armed robbery.”

# FOURTH AMENDMENT AND GEOFENCING

“The questions presented are:

1. Whether the execution of the geofence warrant violated the Fourth Amendment.
2. Whether the exclusionary rule should apply to the evidence derived from the geofence warrant.”

LIMITED TO QUESTION 1 PRESENTED BY THE PETITION.”

- *Chatrie* was argued April 27, 2026.

# FIFTH AMENDMENT

*Fisher v. United States*, 425 U.S. 391 (1976):

"Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena. *Curcio v. United States*, \*\*\*. The elements of compulsion are clearly present, but the more difficult issues are whether the tacit averments of the taxpayer are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment. These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof." 425 U.S. at 410.

# FIFTH AMENDMENT

*United States v. Doe*, 465 U.S. 605 (1984):

“Although the contents of a document may not be privileged, the act of producing the document may be. \*\*\*. A government subpoena compels the holder of the document to perform an act that may have testimonial aspects and an incriminating effect.” 465 U.S. at 612.

# FIFTH AMENDMENT

- *State v. Andrews*, 243 N.J. 447 (2020), cert. denied, No. 20-937 (U.S. May 17, 2021):

Fifth Amendment privilege against self-incrimination did not protect defendant from the compelled disclosure of the passcodes.

- *Seo v. State*, 148 N.E.3d 952 (Ind. 2020):

“law enforcement sought to compel Seo to unlock her cell phone so that it could then scour her device for incriminating information. And Seo’s act of producing her unlocked cell phone would provide the State with information it does not already know.”

# THE SIXTH AMENDMENT AND INEFFECTIVE ASSISTANCE OF COUNSEL

- *People v. Wakefield*, 175 A.D.3d 158, 107 N.Y.S.3d 487 (3d Dept. 2019), *aff'd*, 38 N.Y.3d 367, 195 N.E.3d 19, 174 N.Y.S.3d 312 (2022)
- *United States v. Michel*, Crim. No. 19-148-1 (CKK) (D.D.C. Aug. 30, 2024)

# ADMISSIBILITY IN GENERAL

The “hurdles” to admissibility:

- Is it relevant?
- Is it authenticated?
  - Self-authentication
  - Testimony of competent person?
- Is it hearsay?
  - If it is, is there an exception?
- Is it an original?
- Is there undue prejudice?

# MIGHT AN EXPERT WITNESS BE REQUIRED?

*State v. Knight*, 259 N.J. 407 (2024):

“A key issue raised by both defendants is whether the trial court erred by allowing the jury to observe multiple times, in slow motion and with pauses, an approximately six-second segment of a surveillance video. \*\*\* The trial judge permitted those jury playbacks under her supervision in the courtroom, over defendants' objection.” (from the decision below, 477 N.J. Super. 400 (App. Div. 2023))

# MIGHT AN EXPERT WITNESS BE REQUIRED?

“But some tools or functions may be so specialized that their usage constitutes an alteration of evidence, or the creation of new evidence. If a party intends to play a video with something beyond the ‘basic techniques’, noted in [State v.] Watson, [254 N.J. 558 (2023)], that party must come forward and alert the trial court and opposing counsel to any modifications or alterations made to the evidence. In those situations, a qualified expert may need to testify about the modifications consistent with N.J.R.E. 702. Watson, 254 N.J. at 606 (explaining that an expert would be required to testify about how they ‘enhance[d] the quality of an electronic or video recording,’ or used “more elaborate forensic techniques . . . like ‘pixel tracking’”).”

# MIGHT AN EXPERT WITNESS BE REQUIRED?

*State v. Hannah*, A-44-24, 2026 N.J. LEXIS 378 (Apr. 16, 2026):

“In this appeal, we consider whether a lay witness can testify regarding cell site location information (CSLI) -- specifically, the locations of cell towers that cell phones connect to -- or whether an expert witness is required to provide such testimony.

\*\*\*

For the reasons that follow, we affirm the judgment of the Appellate Division and hold, pursuant to N.J.R.E. 702, that CSLI involves technical and specialized knowledge that must be presented to a jury by an expert witness at trial.”

# ADMISSIBILITY IN FEDERAL COURTS

## Federal Rules of Evidence:

- 104(a) (role of judge and jury)
- 107 (illustrative aids)
- 401 (relevance)
- 402 (admissibility, but \*\*\*)
- 403 (prejudice, etc.)
- 901 and 902 (authenticity)
- 801-808 (hearsay)
- 1002 (“original” requirement)

# FEDERAL RULE OF EVIDENCE 107

## ILLUSTRATIVE AIDS

Rule 107:

“(a) Permitted Uses. The court may allow a party to present an illustrative aid to help the trier of fact understand the evidence or argument if the aid's utility in assisting comprehension is not substantially outweighed by the danger of unfair prejudice, confusing the issues, misleading the jury, undue delay, or wasting time.

(b) Use in Jury Deliberations. An illustrative aid is not evidence and must not be provided to the jury during deliberations unless:

(1) all parties consent; or

(2) the court, for good cause, orders otherwise.

\*\*\*”

# FEDERAL RULE OF EVIDENCE 107

## ILLUSTRATIVE AIDS

From the Committee Notes on Rules—2024:

“The amendment establishes a new Rule 107 to provide standards for the use of illustrative aids. The new rule is derived from Maine Rule of Evidence 616. The term ‘illustrative aid’ is used instead of the term ‘demonstrative evidence,’ as that latter term has been subject to differing interpretation in the courts. An illustrative aid is any presentation offered not as evidence but rather to assist the trier of fact in understanding evidence or argument. ‘Demonstrative evidence’ is a term better applied to substantive evidence offered to prove, by demonstration, a disputed fact.”

# FEDERAL RULE OF EVIDENCE 901

## AUTHENTICATING OR IDENTIFYING EVIDENCE

“(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement:

\*\*\*

(9) *Evidence About a Process or System.* Evidence describing a process or system and showing that it produces an accurate result.”

# REJECTED PROPOSAL TO AMEND RULE 901

There was a proposal to amend Rule 901 to add a new subsection (c). It would have read:

“Potentially Fabricated or Altered Electronic Evidence.

If a party challenging the authenticity of computer-generated or other electronic evidence demonstrates to the court that it is more likely than not either fabricated, or altered in whole or in part, the evidence is admissible only if the proponent demonstrates that its probative value outweighs its prejudicial effect on the party challenging the evidence.”

# REJECTED PROPOSAL TO AMEND RULE 901

The Committee agreed “not to publish proposed Rule 901(c) regarding authentication of evidence potentially generated by AI but to continue developing an appropriate provision in case an emergent need arises to add a rule to keep pace with evolving technology in the courtroom.”

(See pp. 92-99 for discussion of “Proposed Amendments to Address Machine-Generated Evidence and Artificial Intelligence,”

<https://www.uscourts.gov/sites/default/files/document/2025-06-standing-agenda-book.pdf>)

# PROPOSAL TO AMEND FEDERAL ADMISSIBILITY RULES

On June 10, 2025, the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States voted to publish a new federal rule of evidence:

“Rule 707. Machine-Generated Evidence

When machine-generated evidence is offered without an expert witness and would be subject to Rule 702 if testified to by a witness, the court may admit the evidence only if it satisfies the requirements of Rule 702 (a)-(d). This rule does not apply to the output of basic scientific instruments.”

# PROPOSAL TO AMEND FEDERAL ADMISSIBILITY RULES

The Committee Note on Rule 707 includes the following:

“The rule is not intended to encourage parties to opt for machine-generated evidence over live expert witnesses. Indeed the point of the rule is to provide reliability-based protections when a party chooses to proffer machine evidence instead of a live expert.”

(See <https://www.uscourts.gov/forms-rules/proposed-amendments-published-public-comment>)

# CLOSING THOUGHTS

- Electronic information is a common feature of criminal investigations and proceedings. Attorneys and judges should understand constitutional and practical uses and limits on its use.
- The session is intended for any attorney who may use – or respond to – the use of electronic information in criminal matters.
- The biggest “takeaway” is that attorneys should be prepared to use – or challenge the use of -- electronic information.

# RESOURCES

- C. Cwik, P. Grimm, M. Grossman and T. Walsh, “Artificial Intelligence, Trustworthiness, and Litigation.” Artificial Intelligence and the Courts: Materials for Judges” (AAAS 2022), [https://www.aaas.org/sites/default/files/2022-09/Paper%20\\_AI%20and%20Trustworthiness\\_NIST\\_FINAL.pdf](https://www.aaas.org/sites/default/files/2022-09/Paper%20_AI%20and%20Trustworthiness_NIST_FINAL.pdf)
- P.W. Grimm, “New Evidence Rules and Artificial Intelligence,” Litigation (ABA: Sept. 1, 2018), [https://www.americanbar.org/groups/litigation/publications/litigation\\_journal/2018-19/fall/new-evidence-rules-and-artificial-intelligence/](https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/fall/new-evidence-rules-and-artificial-intelligence/)

# RESOURCES

- P. W. Grimm, M.R. Grossman, and G.V. Cormack, “Artificial Intelligence as Evidence,” 19 *Nw. J. Tech. & Intell. Prop.* 9 (2021), <https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2/>
- P.W. Grimm, M.R. Grossman, and K.F. Brady, “Decision Tree for Evaluating AI-Generated Evidence,” 27 *Sedona Conf. J.* \_\_\_\_ (forthcoming 2026), [aiGeneratedEvidence Tree\\_FormattedFinal](#)
- M.R. Grossman & P.W. Grimm, “Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence,” 26 *Colum. Sci. & Tech. L. Rev.* 110 (2025), <https://journals.library.columbia.edu/index.php/stlr/>

# RESOURCES

- R.J. Hedges, “Artificial Intelligence Discovery & Admissibility Case Law and Other Resources” (Jan. 2024 and July 2025) (in materials)
- R.J. Hedges, *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials*,  
<https://www.mass.gov/service-details/understanding-electronic-information-in-criminal-investigations-and-actions>
- R.J. Hedges, *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials* (Apr. 2025) (in materials)

**QUESTIONS?  
COMMENTS?  
THANK YOU!**