Electronic Evidence in Criminal Investigations and Actions:

Representative Court Decisions and Supplementary Materials

Ronald J. Hedges, Editor

Research Assistant: Eric S. McKee

FEBRUARY 2023

Table of Contents

FOREWARD TO THE FEBRUARY 2023 EDITION x

TAGS xi

ABBREVIATIONS xii

DECISIONS – UNITED STATES SUPREME COURT 1

Counterman v. Colorado, No. 22-138, 2023 WL 178395, *cert.* granted (U.S. Jan. 13, 2023) 1

DECISIONS – FEDERAL 1

Bailey v. Iles, No. 1:20-CV-01211, 2022 WL 2836239 (W.D. La. July 20, 2022) 1

Bowers v. Cnty. of Taylor, 598 F. Supp. 3d 719 (W.D. Wis. 2022) 2

Brennan v. Dickson, 45 F.4th 48 (D.C. Cir. 2022) 3

Lindell v. United States, No. 22-CV-2290 (ECT/ECW), 2022 WL 16647786 (D. Minn. Nov. 3, 2022) 4

Malik v. U.S. Dep't of Homeland Sec., No. 4:21-CV-0088-P, 2022 WL 3104840 (N.D. Tex. Aug. 4, 2022) 5

Novak v. City of Parma, 33 F.4th 296 (6th Cir. 2022) 6

Sanchez v. Los Angeles Dep't of Transportation, 39 F.4th 548 (9th Cir. 2022) (amended opinion) (Summary) 7

Matter of O'Donovan, No. 22-MJ-1000-DLC, 2022 WL 10483922 (D. Mass. Oct. 17, 2022) 9

In re Sittenfeld, 49 F.4th 1061 (6th Cir. 2022) 10

Trump v. United States, No. 22-13005, 2022 WL 4366684 (11th Cir. Sept. 21, 2022) (*per curiam*)*, app. to vacate stay denied, Trump v. United States,* 214 L. Ed. 2d 166, 143 S. Ct. 349 *(2022*) 10

Trump v. United States, 54 F.4th 689 (11th Cir. 2022) (*per curiam*) 11

United States v. Bledsoe, No. CR 21-204 (BAH), 2022 WL 3594628 (D.D.C. Aug. 22, 2022) ... 12

United States v. Graham, 47 F.4th 561 (7th Cir. 2022) 14

United States v. Knight, No. 21-10197, 2023 WL 34698 (9th Cir. Jan. 4, 2023) 15

United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (*en banc*) 15

United States v. Morton, 46 F.4th 331 (5th Cir. 2022) (*en banc*) 18

United States v. Phillips, 32 F.4th 865 (9th Cir.)*, (cert. denied),* 143 S. Ct. 467 (2022) 18

United States v. Rosenow, 50 F.4th 715 (9th Cir. 2022) (9th Cir. Filed Apr. 27, 2022; amended Oct. 3, 2022) (Summary of Sections of Amended Decision and Dissent) 19

United States v. Rhine, Criminal Action No. 21-0687 (RC) (D.D.C. Jan. 24, 2023) 21

United States v. Taylor, 54 F.4th 795 (4th Cir. 2022) 22

United States v. Wiley, No. 3:21CR98 (JBA), 2022 WL 2656788 (D. Conn. July 8, 2022) 22

United States v. Yung, 37 F.4th 70 (3d Cir. 2022) 23

Matter of Use of A Cell-Site Simulator to Identify a Cellular Device in a Narcotics Trafficking Case, No. 22 M 615, 2022 WL 3645982 (N.D. Ill. Aug. 24, 2022) 24

DECISIONS – STATE 24

Commonwealth v. DeJesus, 489 Mass. 292, 182 N.E.3d 280 (2022) 24

Commonwealth v. Perry, 489 Mass. 436, 184 N.E.3d 745 (2022) 26

Owner Operator Indep. Drivers Ass'n, Inc. v. New York State Dep't of Transportation, 205 A.D.3d 53, 166 N.Y.S.3d 337 (2022) 31

Irwin Indus. Tool Co. v. Pifer, 478 Md. 645, 276 A.3d 533 (2022) 33

Long Lake Twp. v. Maxon, No. 349230, 2022 WL 4281509 (Mich. Ct. App. Sept. 15, 2022) 33

People v. Alexander, 207 A.D.3d 874, 172 N.Y.S. 3d 516, leave to appeal denied, 39 N.Y.3d 984 (2022) 35

People v. Bullard-daniel, 203 A.D.3d 1630, 163 N.Y.S.3d 726 (2022), lv. to appeal denied, 38 N.Y.3d 1069, 171 N.Y.S.3d 444 (2022) 37

People v. Easley, 38 N.Y.3d 1010, 188 N.E.3d 586 (2022)(*mem.*) 38

People v. Licona-Ortega, 2022 COA 27, 511 P.3d 721, cert. denied, No. 22SC252, 2022 WL 16778997 (Colo. Nov. 7, 2022) 39

People v. McNabb, 2022 IL App (4th) 220070-U (2022) 40

People v. Reedy, 211 A.D.3d 1629 (N.Y. App. Div. 2022) 41

People v. Rodriguez, 38 N.Y.3d 151, 190 N.E.3d 36 (2022) 42

In re J.T., No. H048553, 2022 WL 2865856 (Cal. Ct. App. July 21, 2022), review denied (Oct. 12, 2022) 43

People v. Wakefield, 38 N.Y.3d 367, 195 N.E.3d 19, reargument denied, 38 N.Y.3d 1121, 192 N.E.3d 1152 (2022)*, and cert. denied sub nom. Wakefield v. New York,* 143 S. Ct. 451 (2022) 44

People v. Watts, 2022 IL App (4th) 210590 (2022) 47

I/M/O Search of Information Stored at the Premises Controlled by Google, Feb. 8, 2022, Case No. KM-2022-79 (Va. 19th Jud. Cir. Feb. 24, 2022) 48

State v. Campbell, 2022-Ohio-3626 (2022) 48

State v. Bowers, Appeal No. 2021AP1767-CR, 2022 WL 17984985 (Wis. App., 2022) 49

State v. Garcia, 350 So. 3d 322 (Fla. 2022) 50

State v. C.J.l., 471 N.J. Super. 477, 274 A.3d 611 (App. Div. 2022) 51

State v. O, 514 P.3d 445 (N.M. Sup. 2022) 53

State v. Riley, 170 Idaho 572, 514 P.3d 982 (2022)*, reh'g denied* (Aug. 24, 2022) 54

State v. Watson, 472 N.J. Super. 381, 277 A.3d 39 (App. Div. 2022) 55

Taylor v. Tolbert, 644 S.W.3d 637 (Tex. 2022) 56

DECISIONS AND OTHER "OFFICIAL" – FOREIGN 58

House of Lords, "Technology Rules? The Advent of New Technologies in the Justice System" (Justice and Home Affairs Comm., 1st Report of Session 2021-22: published March 30, 2022) 58

USDOJ, "Joint Statement by the United States and the United Kingdom on Data Access Agreement" (Office of Public Affairs: July 21, 2022), (DOJ 22-784) 58

USDOJ, Office of International Affairs ("OIA") Home Page 58

STATUTES, REGULATIONS, ETC. – FEDERAL 59

Fed. R. Crim. P. 16 amended effective December 1, 2022 59

#Discovery 59

28 CFR Part 201 – Data Protection Review Court 59

#International 59

Federal Bureau of Investigation Training Document, "(U/FOUO FBI's Ability to Legally Access Secure Messaging App Content and Metadata" (Jan. 7, 2021) 59

#Encryption 59

#Fourth Amendment – Warrant Required or Not 59

#Reasonable Expectation of Privacy 59

#SCA 59

Federal Defender Services Office, “San Francisco Police Are Using Driverless Cars as Mobile Surveillance Cameras’ (Training Division: May 20, 2022) 59

Office of the Director of National Intelligence, “Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Surveillance Authorities Calendar Year 2021” (Office of Civil Liberties, Privacy, and Transparency: Apr. 2022) 60

USDHS, “Feature Article: Robot Dogs Take Another Step Towards Deployment at the Border” (Release date: Feb. 1, 2022) 60

USDOJ, “Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement” (Press Release Sept. 15, 2022) 60

USDOJ, “District of Columbia Man Charged with Obstruction of Justice for Illegally Recording and Publishing Grand Jury Proceedings” (United States Attorney’s Office for District of Columbia: Nov. 17, 2022) 61

USDOJ, “Further Revisions to Corporate Enforcement Policies Following Discussions with Corporate Crime Advisory Group” (Office of the Deputy Attorney General: Sept. 15, 2022) 61

#Social Media 61

USDOJ, “Google Enters into Stipulated Agreement to Improve Legal Process Compliance Program” (Press Release: Oct. 25, 2022) 61

#Preservation and Spoliation 61

USDOJ, "Justice Dept. Withdraws Outdated Enforcement Policy Statements" (Office of Public Affairs: Feb. 3, 2023), (DOJ 23-137) 61

USDOJ, “Justice Dept. Announces Report on Digital Assets and Launces Nationwide Network” (Press Release: Sept. 16, 2022) 61

USDOJ, “The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets” (Office of the Attorney General: Sept. 6, 2022) 62

“Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities” (White House: Oct. 7, 2022) 62

STATUTES, REGULATIONS, ETC. – STATE 62

Arizona House Bill 2219, signed into law July 6, 2022, ("Unlawful video recording of law enforcement activity; classification; definition") 62

California Assembly Bill 2799, signed into law Sept. 30, 2022 62

California Senate Bill 1228, signed into law Sept. 30, 2022 63

Idaho Statement of Officer in support of search warrant for deaths at University of Idaho . 64

Office of the Mayor, San Francisco, "Board of Supervisors Approves Camera Access Legislation to Better Protect Residents, Businesses, and Neighborhoods" (Sept. 21, 2022) 64

San Francisco Police Training Document 65

ARTICLES 65

"Apple Advances User Security with Powerful New Data Protections," *Apple Update* (Dec. 7, 2022) 65

K. Basu & S. Witley, "Google—DOJ Settlement Sends Message on Handling Third-Party Data," *Bloomberg Law* (US Law Week: Oct. 27, 2022) 65

A.J. Battaglia, "Changing Tide in Expert Witness Procedures in Criminal Cases." *San Diego FBA* (Nov. 6, 2022) 65

J. Bhuiyan, "Surveillance Shift: San Francisco Pilots Program Allowing Police to Live Monitor Private Security Cameras," *The Guardian* (Oct. 4, 2022) 66

S.J. Bloom, E. Ireland, & J. Knight, "Tips to Follow DOJ Guidance and Survive Corporate Investigations," *Bloomberg Law* (Business & Practice: Jan. 6, 2023) 66

T. Brewster, "The FBI Forced a Suspect to Unlock Amazon's Encrypted App Wickr with Their Face," 66

M. Burgess, "Cops Hacked Thousands of Phones. Was it Legal?" *Wired* (Jan. 4, 2023) 66

R.L. Cassin, "What are the DOJ's 'Other Resources' for Evaluating Corporate Compliance Programs? *The FCPA Blog* (June 2, 2022) 66

Andrew Cohen & O. Kerr, "Could Better Technology Lead to Stronger 4th Amendment Privacy Protections?" (Brennan Center for Justice: Apr. 6, 2022) 67

Cooley Alert, "US-UK Data Access Agreement: Top Five Things to Know" (Sept. 27, 2022) ... 67

J.E. Cutler, "Saving Rape Victims' DNA to Charge Them with Crimes Now Illegal," *Bloomberg Law* (Sept. 30, 2022) 67

B. Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police," *Electronic Frontier Foundation* (Aug. 31, 2022) 67

O. Darcy, "Elon Musk Claims the FBI Paid Twitter to 'Censor Info from the Public.' Here's What the Twitter Files Actually Show," *CNN* (Dec. 20, 2022) 68

R. De, *et al.,* "President Biden Signs Executive Order on U.S. Intelligence Activities to Implement EU-U.S. Data Privacy Framework" (Mayer Brown: Oct. 10, 2022) 68

S. Flynn, "All of Your Messaging App Metadata the FBI Claims It Can Obtain," MUO (Jan. 25, 2022) 68

C. Garvie, "A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations," *Georgetown Law Center on Privacy & Technology* (Dec. 6, 2022) 68

R. Gibbon, *et al,* "Law Enforcement in the Digital Assets Space: Department of Justice Issues Report Pursuant to White House Executive Order," *The* Anticorruption *Blog* (Squire Patton Boggs: Sept. 26, 2022) 68

Aaron Gordon, "San Francisco Police Are Using Driverless Cars as Mobile Surveillance Cameras," *Vice* (May 11, 2022) 69

Allison Grande, "FBI Made 3.4M Warrantless US Date Searches, Report Says," *Law360* (Apr. 29, 2022) 69

"Amazon Gave Ring Doorbell Videos to US Police 11 Times Without Permission," *Guardian* (July 13, 2022) 69

S.M. Hall & E.M. Quattrone, "Post-*Dobbs* Abortion Enforcement: Nebraska Uses Facebook Messages as Evidence," *Commercial Litig. Update* (Epstein Becker Green: Aug. 12, 2022) 70

W.W. Hamel, *et al.,* "Part 1: Cooperation in Government Investigations and Voluntary Self-Disclosure: What to Expect After DOJ's Latest Guidance" (Venable: Oct. 13, 2022) .. 70

M. Harris, "A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet," *WIRED* (Nov. 28, 2022) 70

D. Harwell, "Customs Officials Have Copied Americans' Phone Data at Massive Scale," *Washington Post* (Sept. 15, 2022) 70

T.P. Hogan, "What Are the Ethical Rules for Prosecutors Regarding the Public Release of Videos in Officer-Involved Shootings?" 37 *Crim. Justice* 16 (ABA: Spring 2022) 70

Aselle Ibraimova & A. Splittgerber, "EU-US Data Transfers: A Sigh of Relief?" *Reed Smith Client Alert,* (Jan. 4, 2023) 71

Jones Day Insight, "DOJ Announces Major Changes to Corporate Criminal Enforcement Policies" (Sept. 2022) 71

L.M. Martin, "From Paper to Practice: Questions to Evaluate the Real-World Impact of Your Compliance Program Under DOJ Guidelines," *JDSupra* (Dec. 5, 2022) 71

C. Keene, "Reverse Keyword Searches and Crime," *Lexology* (Aug. 11, 2022) 71

O.S. Kerr, "How Body-Worn Cameras Are Changing Fourth Amendment Law," *The Volokh Conspiracy* (Dec. 21, 2022) 71

O.S. Kerr, "The Ninth Circuit's Stunner in *Rosenow,* and Thoughts on the Way Forward," *The Volokh Forward* (May 13, 2022) 72

B. Krebs, "Hackers Gaining Power of Subpoena via Fake 'Emergency Data Requests," *KrebsonSecurity* (Mar. 29, 2022) 72

N.T. Lee & C. Chin, "Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color," *Brookings* (Apr. 12, 2022) 72

K. McCarthy, "More Evidence of the CFAA Post-Van Buren/hiQ Jurisprudential Anarchy," *Tech. & Marketing Blog* (Aug. 4, 2022) 72

J. Menn, "Apple Says It Will Allow iCloud Backups to be Fully Encrypted," *Washington Post* (Dec. 7, 2022) 73

L.H. Newman, "The Surveillance State is Primed for Criminalized Abortion," *WIRED* (May 24, 2022) 73

K. Owens, *et al.,* "Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives," *USENIX* (paper presented at 31st USENIX Security Symposium) 73

B. Penn, "Evidence Avalanche Prompts Less-Is-More Pivot by US Prosecutors," *Bloomberg Law* (June 15, 2022) 74

K.S. Reimann, "The 2022 DOJ Enforcement Guidance: Areas for Compliance Program Focus," *Program on Corporate Compliance and Enforcement* (NYU School of Law: undated) 74

R. Sanchez, "As Police in Idaho Faced Mounting Criticism, Investigators Worked Meticulously Behind the Scenes to nab a Suspect," *CNN* (Jan. 8, 2023) 74

J.F. Savarese, *et al.,* "DOJ Clarifies Its Policies for Corporate Criminal Enforcement," *Program on Corporate Compliance and Enforcement* (NYU School of Law: undated) 74

J. Schuppe, "Police Sweep Google Searches to Find Suspects. The Tactic is Facing Its First Legal Challenge," *NBC News* (June 30, 2022) 75

F. Siddiqui & J. Menn, "'Hit the Kill Switch': Uber Used Covert Tech to Thwart Government Raids," *Washington Post* (July 10, 2022) 75

Sidley Update, "Making Sense of DOJ's New Monaco Memo on Corporate Enforcement" (Sept. 21, 2022) 75

P. Stein, "How Agents Get Warrants Like the One Used at Mar-a-Lago, and What They Mean," *Washington Post* (Aug. 11, 2022) 75

Twitter Help Center, "Guidelines for Law Enforcement," (undated) 76

Variety, "Calif. Restricts Use of Rap Lyrics in Criminal Trials After Gov. Newsom Signs Bill," *NBC News* (Sept. 30, 2022) 76

F.S. Venancio de Souza, "Roe v. Wade's Overturn: The Impact of Data Protection and Law Enforcement," *IAPP* (July 1, 2022) 76

Aruna Viswanatha & S. Gurman, "Ample Jan. 6 Evidence Helps Secure High Conviction Rate in Capitol Riot," *Wall. St. J.* (Jan. 2, 2023) 76

Andrea Vittorio, "New Law Buffers California Companies from Abortion Data Requests," *Bloomberg Law* (Sept. 28, 2022) 76

E. Volokh, "Hearsay Evidence Admissible in Gun Violence Restraining Order Proceeding," *The Volokh Conspiracy* (Dec. 19, 2022) 77

FOREWARD TO THE FEBRUARY 2023 EDITION

The first edition of *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials* was published in February 2016. That edition attempted to be a comprehensive collection of case law and materials that provided guidance on how electronic information featured in criminal investigations and proceedings. Later supplements followed the first edition and, in December of 2017, a new edition was published that incorporated everything into a single compilation. Thereafter, in September 2019, August 2020, April 2021, and April 2022, editions were published that updated the compilation. The time has come to publish yet another update.

This latest supplement features links to materials, as does its predecessors. The links here were last visited when the supplement was completed in January of 2023. The reader is cautioned that specific links may have become stale over time. Note also that I have included some decisions that are not "criminal" in nature but that might be related to regulatory actions or be civil in nature. The substantive nature of these decisions might bear on, for example, Fourth Amendment rights.

Now, a personal note: I began this undertaking with the intent of selecting a handful of decisions to illustrate how electronic information has impacted criminal law and procedure. Why? We live at a time when electronic information is "everywhere" and comes in many shapes and sizes or, put in other words, ever-increasing volumes, varieties, and velocities. As with every other product of the human imagination, electronic information can be used for good or bad. Those uses raise many issues in the context of criminal investigations and proceedings and electronic information is now a common feature in the commission, investigation, and prosecution of crimes. Among other things, those issues present questions of how the Bill of Rights and equivalent State constitutional guarantees apply to electronic information. Moreover, new sources of electronic information and technologies appear on a seemingly daily basis and must be "fitted" into constitutional and statutory frameworks. I hope that this new supplement, along with its predecessors, will inform the groups of actors in the criminal justice system, whether judicial, law enforcement, prosecution, defense,

or support, on how issues arising out of electronic information might be presented and resolved.

Every edition has been posted on the website of the Massachusetts Attorney General's Office. I want to thank that agency for allowing the postings. I also want to extend specific thanks to, among others, Chris Kelly, for making the postings possible.

I also want to extend special thanks to Eric McKee, who reviewed and edited this compilation. Mr. McKee is a graduating student from Rutgers Law School and is a member of the Rutgers Student Bar Association, where he serves as a third-year student representative. Mr. McKee is also a member of the Federalist Society and serves as the Vice President of the Rutgers Law Newark Chapter.

TAGS

#Admissibility

#CSLI

#Discovery Materials

#Encryption

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Ex Ante Conditions

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

#Preservation and Spoliation

#Probation and Supervised Release

#Reasonable Expectation of Privacy

#Sixth Amendment – Assistance of Counsel

#Sixth Amendment – Right of Confrontation

#SCA (Stored Communications Act)

#Social Media

#Third-Party Doctrine

#Trial-Related

ABBREVIATIONS

“Cell Site Location Information” – CSLI

“Stored Communications Act” – SCA

DECISIONS – UNITED STATES SUPREME COURT

Counterman v. Colorado, No. 22-138, 2023 WL 178395, *cert.* granted (U.S. Jan. 13, 2023)

Question Presented: Whether, to establish that a statement is a "true threat" unprotected by the First Amendment, the government must show that the speaker subjectively knew or intended the threatening nature of the statement, or whether it is enough to show that an objective "reasonable person" would regard the statement as a threat of violence.

#Miscellaneous

#Social Media

DECISIONS – FEDERAL

Bailey v. Iles, No. 1:20-CV-01211, 2022 WL 2836239 (W.D. La. July 20, 2022)

This civil action arose out of a posting by the plaintiff on Facebook. The plaintiff claimed that the posting was intended to be a joke. However, local law enforcement took it to be a threat to public safety and arrested the plaintiff, although the local prosecutor declined to prosecute. Plaintiff then brought a Section 1983 action against various officers. The district court granted summary judgement in the defendants' favor because, among other things, (1) Probable cause existed for the plaintiff's arrest and therefore the individual who investigated the posting and qualified immunity under the Fourth Amendment, and (2) the posting constituted a clear and present danger and therefore it had no First Amendment protection.

#Miscellaneous

#Social Media

Bowers v. Cnty. of Taylor, 598 F. Supp. 3d 719 (W.D. Wis. 2022) "This case arises from a government agency's search of an online account by one of its employees. It poses close questions of Fourth Amendment law concerning online accounts and the rights of public employees." The plaintiff was a sergeant in the defendant sheriff's office. As part of an investigation into the sharing of files with a television show, the sheriff's IT director was able to access the plaintiff's personal Dropbox account, which was linked to his work email. The director changed the plaintiff's account password, accessed the account, and found the files. The plaintiff brought this Section 1983 action, alleging that the defendants had violated the Fourth Amendment by accessing the account without a warrant. The court awarded summary judgement to the defendants:

> The general rule is that a warrant is required for searches of private property. But there are more lenient standards involving some searches conducted by government employers. The Dropbox account was Bowers's personal account, and it wasn't stored on county servers, factors tending to support Bowers's contention that a warrant was required. But other factors point the other way, including that Bowers linked the account to his work email and he placed work files taken from a work computer into the account. The account was password protected, but Bowers had shared access with several others.
>
> In the court's view, defendants' search was distinct from a typical workplace search, and the Dropbox account was sufficiently private to fall within the general warrant requirement. But the court reaches that conclusion only by extending principles from current precedent and following the reasoning of courts from other circuits. Bowers hasn't cited analogous cases from the Supreme Court or the Court of Appeals for the Seventh Circuit, and the more general case law he cites doesn't apply with obvious clarity to his situation. Under these circumstances, defendants did not violate any clearly established rights, and thus they are entitled to qualified immunity. The court will grant their motion for summary judgment.

[The facts of this decision are the same as State v. Bowers, digested below. Different issues before different courts.]

Fourth Amendment – Good Faith Exception

Fourth Amendment – Warrant Required or Not

Brennan v. Dickson, 45 F.4th 48 (D.C. Cir. 2022)

This was a challenge to the Remote Identification Rule promulgated by the FAA to regulate drone use in U.S. airspace. As described by the appellate court,

Like a license plate, Remote ID acts as a basic building block of regulatory compliance by attaching a unique, visible, yet generally anonymous identifier to each device in public circulation. Unlike a license plate on the back of a car, however, Remote ID is detectible in real time only when the drone is moving. Also unlike a vehicle's license plate, which can only be read by the naked eye from a few yards away, a Remote ID message can be 'read' by people within range of local radio signals yet not near enough even to see the drone itself.

The FAA separately obtains certain nonpublic personally identifying information from drone owners as a requisite of their unmanned aircraft registrations, and that information is protected by the Privacy Act ***. A Remote ID message may only be matched to that nonpublic information and used by the FAA or disclosed to law enforcement outside of the FAA 'when necessary and relevant to a[n] FAA enforcement activity,' ***. and even then it is subject to 'all due process and other legal and constitutional requirements,'***. The Rule does not otherwise authorize private or public actors access to drone owners' or pilots' nonpublic personally identifying information ***, nor does it permit or contemplate storage of Remote ID data for subsequent record searches.

The Court of Appeals upheld the rule. Summarizing its discussion of the constitutional challenge, the court held:

Petitioners Tyler Brennan *** want the Rule vacated. Brennan asserts that the Rule's Remote ID requirement amounts to constant, warrantless

governmental surveillance in violation of the Fourth Amendment. His request for vacatur of the Rule, amounting to a facial challenge, must fail because drones are virtually always flown in public. Requiring a drone to show its location and that of its operator while the drone is aloft in the open air violates no reasonable expectation of privacy. Brennan hypothesizes that law enforcement authorities could use Remote ID to carry out continuous surveillance of drone pilots' public locations amounting to a constitutionally cognizable search, or that the Rule could be applied in ways that would reveal an operator's identity and location at a home or in an otherwise private place. But he has not shown that any such uses of Remote ID have either harmed him or imminently will do so, thus he presents no currently justiciable, as-applied challenge. [citations omitted].

#Fourth Amendment: Warrant Required or Not

#Reasonable Expectation of Privacy

Lindell v. United States, No. 22-CV-2290 (ECT/ECW), 2022 WL 16647786 (D. Minn. Nov. 3, 2022)

This action arose out of a seizure of a cell phone pursuant to a search warrant which took place while the individual plaintiff was in the drive-through lane of a restaurant. The plaintiffs sought access to warrant application materials. They also sought preliminary injunctive relief pursuant to, among other things, *Fed. R. Crim. P.* 41(g) for return of the phone and to prohibit the Government from using any information retrieved from the phone. The district court denied the motions. It found, among other things, that the Government had demonstrated compelling reasons (an ongoing investigation and protection of the interests of untargeted persons) to keep the materials sealed at the pre-indictment stage. The court also found that the plaintiffs had not shown a likelihood of success on the merits or irreparable harm, thus foreclosing injunctive relief.

#Miscellaneous

Malik v. U.S. Dep't of Homeland Sec., No. 4:21-CV-0088-P, 2022 WL 3104840 (N.D. Tex. Aug. 4, 2022)

The plaintiff was "flagged" for a "secondary" inspection when he entered the United States at Dallas--Fort Worth Airport on his return from Costa Rica. The plaintiff, an attorney, refused to consent to a "basic" search of his cell phone on the ground of attorney-client privilege. His phone was then detained and sent to a lab, where the password was bypassed and the phone data was accessed and sent to Customs and Border Protection (CBP). CBP assembled a filter team to redact privileged material. A "limited set" of data was then sent to CBP at the airport, which conducted a border search of the data and then returned the phone to the plaintiff. Plaintiff brought this action, alleging that the seizure and search violated his First and Fourth Amendment rights. On cross-motions for summary judgment, the district court held, among other things, that the plaintiff lacked standing to sue for declaratory relief because his allegations went to retrospective—and not prospective—injury and, even assuming that the defendants had violated the plaintiff's rights, the Government could not be compelled to destroy any data seized as, "[o]utside the context of a criminal trial, the Government is generally free to use evidence obtained in an unlawful search." The district court did find that the plaintiff had standing to pursue an expungement remedy because the Government had retained the data when the plaintiff requested a litigation hold. However, under the border search exception to the Warrant Requirement, the Government demonstrated "reasonable suspicion" for its nonroutine border search and, accordingly, there was no Fourth Amendment violation when the phone was seized. The district court also granted summary judgement on the plaintiff's First Amendment claim, concluding that there was no First Amendment exception to the Fourth Amendment border search doctrine.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Preservation and Spoliation

Novak v. City of Parma, 33 F.4th 296 (6th Cir. 2022)

The plaintiff in this Section 1983 action created a Facebook page that looked like that of the defendant City. He thought it would be funny. The plaintiff was arrested and prosecuted under an Ohio law for using a computer to disrupt police functions. He was indicted and acquitted. Here, the Sixth Circuit Court of Appeals affirmed the entry of summary judgment in favor of various officers. It held, among other things, that there was probable cause to believe that the plaintiff had violated the law and that the officers were entitled to qualified immunity for Amendment and Fourth Amendment claims. The appellate court also rejected the plaintiff's claim that the actions of the officers did not constitute an unconstitutional prior restraint. The court concluded with *dicta*:

> Little did Anthony Novak know when he launched 'The City of Parma Police Department' page that he'd wind up a defendant in court. So too for the officers who arrested him. At the end of the day, neither got all they wanted—Novak won't be punished for his alleged crime, and the defendants are entitled to summary judgment on Novak's civil claims.
>
> But granting the officers qualified immunity does not mean their actions were justified or should be condoned. Indeed, it is cases like these when government officials have a particular obligation to act reasonably. Was Novak's Facebook page worth a criminal prosecution, two appeals, and countless hours of Novak's and the government's time? We have our doubts. And from the beginning, any one of the officials involved could have allowed 'the entire story to turn out differently,' simply by saying 'No.' ***. Unfortunately, no one did.

#Miscellaneous

#Fourth Amendment – Good Faith Exception

#Social Media

Sanchez v. Los Angeles Dep't of Transportation, 39 F.4th 548 (9th Cir. 2022) (amended opinion) (Summary)

The panel amended its prior opinion affirming the district court's order dismissing, for failure to state a claim, an action brought by an e-scooter user alleging that the City of Los Angeles' e-scooter permitting program, which requires e-scooter companies to disclose real-time location data for every device, violates the Fourth Amendment and California law.

As a condition of getting a permit, the Los Angeles Department of Transportation ('LADOT') required escooter operators to provide vehicle location data through an application programming interface called Mobility Data Specification ('MDS'). Used in conjunction with the operators' smartphone applications, MDS automatically compiles real-time data on each e-scooter's location by collecting the start and end points and times of each ride taken.

The complaint alleged that the MDS protocols provide the location of e-scooters with Orwellian precision. A City therefore allegedly could easily use MDS data in conjunction with other information to identify trips by individuals to sensitive locations. Because the location data could be preserved in accordance with LADOT data-retention policies, plaintiff alleged that the City could travel back in time to retrace a rider's whereabouts.

The panel first held that plaintiff's complaint alleged facts giving rise to Article III standing and therefore the panel rejected LADOT's assertion that the complaint was beyond the panel's constitutional purview because it was premised on a hypothetical invasion of privacy that might never occur. Drawing all reasonable inferences in favor of plaintiff as it was required to do at the Fed. R. Civ. P. 12(b)(6) stage, the proper reading of the complaint was that plaintiff alleged that the collection of the MDS location data itself—without more—violated his constitutional rights.

The panel concluded that the third-party doctrine, which provides that a person has no legitimate expectation of privacy in information he voluntarily

turns over to third parties, foreclosed plaintiff's claim of a reasonable expectation of privacy over the MDS data. Focusing first on 'voluntary exposure,' the panel had little difficulty finding that plaintiff knowingly and voluntarily disclosed location data to the e-scooter operators. Unlike a cell phone user, whose device provides location information by dint of its operation, without any affirmative act on the part of the user, plaintiff affirmatively chose to disclose location data to escooter operators each time he rented a device. Having voluntarily conveyed his location to the operator in the ordinary course of business, plaintiff could not assert a reasonable expectation of privacy.

The panel next determined that the nature of MDS location data indicated a diminished expectation of privacy. The data only discloses the location of an e-scooter owned by the operator and typically rerented to a new user after each individual trip. It was thus quite different than the information generated by a cell phone, which identifies the location of a particular user virtually continuously. The complaint admitted that the MDS data could not be linked to a particular individual without more. Although the Supreme Court has rejected the proposition that inference insulates a search, there was no allegation that the MDS data was in fact used to infer the identity of any individual rider.

The panel held that because the third-party doctrine squarely applied to plaintiff's voluntary agreement to provide location data to the e-scooter operators, the collection of that data by LADOT was not a search and did not violate the Fourth Amendment or the California Constitution. The panel cautioned that its decision was narrow and expressed no view on matters not before the panel, including the result if the MDS data were alleged to have been shared with law enforcement or used to infer individual riders' identities or locations.

The panel affirmed the district court's dismissal of plaintiff's claim under the California Electronic Communications Privacy Act ('CalECPA') on the grounds that the statute did not provide plaintiff with authorization to bring an independent action to enforce its provisions.

Finally, the panel held that the district court did not err in dismissing the complaint without leave to amend. Because plaintiff had no reasonable expectation of privacy over the MDS location data, no additional facts could possibly have cured the deficiency with his constitutional claims. And, because

the court rightly found that the CalECPA did not create a private right of action, dismissal of the statutory claim was also not error.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Third-Party Doctrine

Matter of O'Donovan, No. 22-MJ-1000-DLC, 2022 WL 10483922 (D. Mass. Oct. 17, 2022)

The Government seized a cell phone of an attorney pursuant to a search warrant. Thereafter, he was indicted. In its application for the warrant the Government proposed a protocol that would establish a filter team to identify privileged or potentially privileged materials and set these aside for judicial review to determine if any could be turned over to investigators. The attorney moved to vacate and replace the proposed protocol with one in which he would make initial privilege determinations and identify any privileged materials on a privilege log which the Government could then challenge. After the motion was filed the Government proposed a modified protocol and conferred with the attorney but could not resolve all remaining disputes. The magistrate judge approved the Government's modified proposal for the following reasons, among others: (1) It provided for a FBI forensic analyst not associated with the investigators or the filter team to run the data on the phone through search terms and segregate responsive materials, returning nonresponsive materials to the attorney and allowing the filter team to review responsive ones; (2) the use of a filter team was unlikely to intrude on attorney-client privilege and would not improperly delegate the judicial function to the team; and (3) the risk of inadvertent or improper disclosure of privileged materials to the investigators was minimal.

#Miscellaneous

In re Sittenfeld, 49 F.4th 1061 (6th Cir. 2022)

Alexander Sittenfeld, a criminal defendant convicted by a jury in the district court, has filed a motion in this court to compel a forensic examination of a juror's cellphone, computer, or "any electronic device that [the juror] used to make electronic communications." Sittenfeld presented this same motion to the district court, which denied it. ***. We construe Sittenfeld's motion as an appeal from that order.

Sittenfeld's argument prompted a precursor question that had not been addressed, so we asked for additional briefing on this question: What legal authority empowers a court to order a juror to provide his or her cellphone, computer, or other electronic devices to the court for it to conduct-or permit a party to conduct-a search or forensic examination of the juror's devices?

Because a court's inherent or statutory authority in conducting a *Remmer* [*v. United States*, 347 U.S. 227 (1954)], hearing does not include an unlimited, inquisitorial power to order jurors to surrender their personal possessions, such as their electronic devices, or to divulge their passwords, we hold that the district court had no power to order a forensic examination of the juror's devices. Therefore, we AFFIRM the district court's denial of Sittenfeld's motion and alert the district court that any further aspects of the *Remmer* hearing must comply with this opinion. [footnote omitted].

#Miscellaneous

#Trial-Related

Trump v. United States, No. 22-13005, 2022 WL 4366684 (11th Cir. Sept. 21, 2022) (*per curiam*), app. to vacate stay denied, *Trump v. United States*, 214 L. Ed. 2d 166, 143 S. Ct. 349 (2022)

After the execution of a search warrant at the residence of former President Trump, the district court granted his motion for the appointment of a special master to review seized documents. The Government moved for a partial stay of the district court's order as it

related to certain documents that bore "classification markings." The Eleventh Circuit granted the stay. In so doing, the appellate court emphasized the limited scope of its review. It applied the test adopted in *Richey v. Smith,* 515 F.2d 1239 (5th Cir 1975) which "outlin[ed] the standard for entertaining a pre-indictment motion for the return of property under Rule 41(g)" and concluded that the Government was "substantially likely to succeed in showing that the district court abused its discretion in exercising jurisdiction over Plaintiff's motion as it concerns the classified documents."

#Miscellaneous

Trump v. United States, 54 F.4th 689 (11th Cir. 2022) (*per curiam*)

This appeal requires us to consider whether the district court had jurisdiction to block the United States from using lawfully seized records in a criminal investigation. The answer is no.

Former President Donald J. Trump brought a civil action seeking an injunction against the government after it executed a search warrant at his Mar-a-Lago residence. He argues that a court-mandated special master review process is necessary because the government's Privilege Review Team protocols were inadequate, because various seized documents are protected by executive or attorney-client privilege, because he could have declassified documents or designated them as personal rather than presidential records, and-if all that fails-because the government's appeal was procedurally deficient. The government disagrees with each contention.

These disputes ignore one fundamental question-whether the district court had the power to hear the case. After all: 'Federal courts are courts of limited jurisdiction. They possess only that power authorized by Constitution and statute, which is not to be expanded by judicial decree.' *Kokkonen v. Guardian Life Ins. Co. of Am.,* 511 U.S. 375, 377 (1994) (citation omitted).

This case was such an expansion. Exercises of equitable jurisdiction-which the district court invoked here-should be 'exceptional' and 'anomalous.' ***. Our precedents have limited this jurisdiction with a four-factor test. Richey v. Smith,

515 F.2d 1239, 1243-44 (5th Cir. 1975). Plaintiff's jurisdictional arguments fail all four factors.

In considering these arguments, we are faced with a choice: apply our usual test; drastically expand the availability of equitable jurisdiction for every subject of a search warrant; or carve out an unprecedented exception in our law for former presidents. We choose the first option. So the case must be dismissed.

#Miscellaneous

United States v. Bledsoe, No. CR 21-204 (BAH), 2022 WL 3594628 (D.D.C. Aug. 22, 2022)

After the January 6, 2021, storming of the Capitol, the FBI sought "Facebook identification information for accounts using its platform to broadcast videos *** that were live-streamed or uploaded to Facebook while the account user was physically present" during the insurrection. That information led to the issuance of search warrants which required Facebook to disclose records and content of account owners, including the defendant. He was convicted of various crimes related to January 6th. The district court denied a pretrial defense motion to suppress all evidence from the non-public portions of his Facebook and Instagram accounts. This opinion set forth the court's reasoning.

As framed by the district court,

> the key question presented in this case is whether, under *Carpenter*, the government's acquisition from Facebook of non-content information derived from user-generated content of a highly public event that reveals the user's location, *i.e.,* user-generated location information ('UGLI'), was a Fourth Amendment search requiring a probable cause warrant.

The court concluded that there was no "search" related to Facebook's disclosure of account information because the defendant had voluntarily created social media accounts:

Thus, unlike the CSLI data at issue in *Carpenter* [*v. United States,* 138 S. Ct. 2206 (2018)], the only way that Facebook was able to determine when and where a user engaged in account activity on January 6, 2021, is by virtue of the user making an affirmative and voluntary choice to download the Facebook or Instagram application onto an electronic device, create an account on the Facebook or Instagram platform, and, critically, take no available steps to avoid disclosing his location, before purposefully initiating the activity of live-streaming or uploading a video of a highly public event, in a manner that occurs during the normal course of using Facebook as intended. Defendant has not identified a single instance where Facebook logs information concerning his account activity of posting any photo or video content on the Facebook platform without user action.

Not only has defendant failed to show the UGLI collected by Facebook is automatic and inescapable, but he has also failed to show that Facebook usage is essential to modern life. Defendant has not attempted to place into the record any evidence establishing that Facebook 'and the services [it] provide[s] are 'such a pervasive and insistent part of daily life' that [using] [its social media platform] is indispensable to participation in a modern society.' ***. [citation omitted].

The district court also found that probable cause existed for the issuance of a warrant for the content of his Facebook account:

Based on Facebook's identifications, law enforcement had a solid basis and good reason to believe that the identified social media accounts would contain incriminating information relevant to the crimes committed during the attack on the Capitol on January 6, especially as news footage of the attack showed rioters taking photos and videos of themselves and others breaking into the Capitol, damaging and stealing property from within the building, and attacking law enforcement as the mob impeded the certification of the Electoral College vote. ***. In sum, the issuing judge had a reasonable basis to conclude that evidence of criminal activity occurring during January 6, 2021, would be found in the social media accounts identified by Facebook. [footnote omitted].

The court also concluded that, even if probable cause was lacking, the good faith exception to the Warrant Requirement would apply.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Social Media

#Third-Party Doctrine

United States v. Graham, 47 F.4th 561 (7th Cir. 2022)

The defendant was convicted for conspiracy to commit sex trafficking and related crimes. He appealed from the admission into evidence of footage from a police body camera taken about a year before the defendant was indicted which depicted a confrontation between himself and a coconspirator during which the coconspirator made statements that incriminated the defendant. The coconspirator plead guilty and was listed as a Government witness but did not testify. The defendant moved for a mistrial, arguing that there was a violation of his rights under the Confrontation Clause by the use of the footage. The district court agreed that the Clause had been violated but gave a curative instruction. The Seventh Circuit affirmed the convictions:

> There was no Confrontation Clause violation. Moore uttered her statements spontaneously as the officers were responding to a fight in progress and to rapidly evolving circumstances suggesting that sex trafficking might be occurring at the motel. When statements are made to law-enforcement officers under circumstances objectively indicating that the primary purpose of the police encounter is to respond to an ongoing emergency, the statements are not testimonial and thus do not implicate the Confrontation Clause. That is the case here. And even if a confrontation violation had occurred, it was harmless.

#Admissibility

#Sixth Amendment – Right of Confrontation

United States v. Knight, No. 21-10197, 2023 WL 34698 (9th Cir. Jan. 4, 2023)

The defendant was convicted of two robberies. He argued on appeal, among other things addressed in a separate opinion, that his convictions should be vacated because the district court had erred by permitting a juror to participate remotely in the first two days of the trial. The Ninth Circuit affirmed, holding that the error (assuming there was one) was not "structural" because it had not rendered the trial unfair or the judgment unreliable. It also held that the defendant had made a knowing and voluntary waiver of his right to have the juror present in-person.

#Trial-Related

United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (*en banc*)

The defendants in these consolidated appeals had been under "continuous and surreptitious recording, day and night for eight months, of all the activities in the front curtilage of a private residence visible to a remotely-controlled digital video camera affixed to a utility pole across the street from that residence." The district court had granted the defendants' motions to suppress evidence derived from the surveillance. A panel of the First Circuit reversed. In a *per curiam* order, the *en banc* court unanimously reversed the district court and remanded with instructions to deny the motions. The circuit judges differed in their reasoning.

Three judges held that there had been a "search:"

> As we will explain, we conclude -- unlike our colleagues -- that the government did conduct a Fourth Amendment 'search' when it accessed the digital video record that law enforcement had created over the course of the eight months in question, notwithstanding the government's contention that the record itself is merely a compendium of images of what had been exposed to

public view. As we also will explain, however, we agree with our colleagues that the District Court's order granting the defendants' motions to suppress must be reversed.

We come to that latter conclusion because the relevant controlling precedent from our circuit that was in place at the time that the government drew upon the pole-camera surveillance was United States v. Bucci, 582 F.3d 108 (1st Cir. 2009). And, there, a panel of this court had held that the use by law enforcement of uncannily similar pole-camera surveillance did not constitute a search within the meaning of the Fourth Amendment and so raised no Fourth Amendment concerns. Id. at 116-17. Thus, while we conclude -- unlike our colleagues -- that subsequent developments in Fourth Amendment jurisprudence support the overruling of Bucci and the conclusion that the government conducted a search here, we also conclude that, under the 'good faith' exception to the Fourth Amendment's warrant requirement ***, the government was entitled to rely on Bucci in acting as it did ***.

The result is that our court is unanimous in holding that the District Court's order granting the motions to suppress must be reversed. Our court's rationale for that holding, however, is most decidedly not.

The three of us who join this separate opinion would reverse the District Court's order granting the defendants' motions to suppress based solely on the 'good faith' exception to the Fourth Amendment's warrant requirement. We reject, however, our colleagues' view that the accessing by law enforcement in a criminal case of the record created by the kind of suspicionless, long-term digital video surveillance at issue here does not constitute a Fourth Amendment search.

Mindful of the brave new world that the routine use of such all-encompassing, long-term video surveillance of the front curtilage of a home could bring about, we are convinced that the government does conduct a search within the meaning of the Fourth Amendment when it accesses the record that it creates through surveillance of that kind and thus that law enforcement, in doing so, must comply with that Amendment's limitations. For, in accord with post- Bucci precedents from the Supreme Court of the United States that recognize the effect that the pace of technological change can have on long assumed expectations of privacy, we are convinced that no other conclusion would be faithful to the

balance that the Fourth Amendment strikes between the right to be 'secure' in one's home and the need for public order. [(footnote omitted) (citations omitted in part)].

Three other judges held that had not been a "search:"

Law enforcement installed without a warrant, as the law permits, a camera on a utility pole on a public street to further an investigation into illegal drug and firearms dealing from a house. The camera provided a view of certain portions of the exterior of the front of the house, though not the front door, and the driveway and garage door. All of these views were totally exposed to public observation. The camera produced evidence of criminal activity by the residents of this house from this outside view in a residential neighborhood.

The actions of the law enforcement officers did not, contrary to Chief Judge Barron's concurrence ***, violate the Fourth Amendment. The concurrence, purporting to rely on Carpenter v. United States, —— U.S. ——, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018), wrongly applies that precedent. Carpenter forbids and does not support the concurrence's contention that the use of the video taken from the pole camera by the prosecution violated the Fourth Amendment. The concurring opinion contradicts a fundamental Fourth Amendment doctrine enshrined in the Constitution from the founding, as recognized by Justice Scalia in Kyllo v. United States ***. This concurring opinion would, were it a majority opinion, have unfortunate practical ramifications. [citations omitted in part].

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

[NB: The above is a sufficient recap of 129 pages of "disagreement" about the scope of Carpenter and its application to a specific technology. I will leave more in-depth analysis for another venue or venues.]

United States v. Morton, 46 F.4th 331 (5th Cir. 2022) (*en banc*)
Subsequent History: Petition for Certiorari Docketed by Brian Matthew *Morton v. United States*

The defendant entered a conditional guilty plea to receipt of child pornography and appealed from the denial of his motion to suppress evidence derived from the search of three cell phones. The phones had been seized during the search of his van, which had been pulled over for a traffic stop. Police officers smelled marijuana, arrested the defendant, searched the van, and found evidence of other drugs as well as possible evidence that the defendant was a child predator. Thereafter, a State judge issued warrants to search the phones for evidence of illegal drug activity relying on language in the supporting affidavit that criminals sometimes use phones to engage in that activity. State investigators found evidence of child pornography when they began to search, stopped searching, and secured new warrants. On appeal, a majority of the *en banc* court held that officers were entitled to rely in good faith on the warrants although the affidavit was "borderline." Several judges concurred in the judgement on good faith grounds but questioned whether probable cause existed. Two judges dissented, concluding there was no probable cause and that the affidavit was so "bare bones" as to preclude good faith reliance.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Phillips, 32 F.4th 865 (9th Cir.)*, (cert. denied),* 143 S. Ct. 467 (2022)

The defendant entered a conditional plea to possession of child pornography and appealed the denial of his motion to suppress evidence found on his laptop. The evidence had been found by the

defendant's ex-fiancée, who conducted a private search. She brought the laptop to a sheriff's office, where she showed images she had already viewed to an officer. The officer then seized the laptop and secured a warrant to search its content. The Ninth Circuit affirmed the denial of the motion to suppress. It assumed that there had been a Government search when the ex-fiancée accessed the laptop at the office. Nevertheless, because that search merely "mimicked" the earlier private one, the search was permissible.

#Fourth Amendment – Warrant Required or Not

United States v. Rosenow, 50 F.4th 715 (9th Cir. 2022) (9th Cir. Filed Apr. 27, 2022; amended Oct. 3, 2022) (Summary of Sections of Amended Decision and Dissent)

The panel amended its Opinion filed April 27, 2022, affirming a conviction and sentence on one count of attempted sexual exploitation of a child, 18 U.S.C. § 2251(c), and one count of possession of sexually explicit images of children, 18 U.S.C. § 2252(a)(4)(B), in a case in which the defendant was arrested returning from the Philippines where he engaged in sex tourism involving minors.

The defendant arranged these illegal activities through online messaging services provided by electronic service providers (ESPs) Yahoo and Facebook. His participation in foreign child sex tourism was initially discovered after Yahoo investigated numerous user accounts that Yahoo suspected were involved in child exploitation.

The defendant argued that the evidence seized from his electrical devices upon his arrest should have been suppressed because Yahoo and Facebook were acting as government agents when they searched his online accounts. The panel rejected the defendant's arguments (1) that two federal statutes—the Stored Communications Act and the Protect Our Children Act—transformed the ESPs' searches into governmental action, and (2) that the government was sufficiently involved in the ESPs' searches of the defendant's accounts to trigger Fourth Amendment protection.

The defendant argued that the government's requests pursuant to 18 U.S.C. § 2703(f) directing Yahoo and Facebook to preserve records related to his private communications were an unconstitutional seizure of his property and, as a result, the evidence used to convict him was improperly obtained and his convictions should be reversed. The panel declined to reach the question of whether these preservation requests implicate the Fourth Amendment, because even assuming that they do, there is no basis for suppression given that the record establishes that the ESPs' preservation of the defendant's digital data had no effect on the government's ability to obtain the evidence that convicted him.

The defendant argued that because subpoenas to Facebook for the defendant's basic subscriber and IP information under 18 U.S.C. § 2703(c)(2) were issued without a warrant supported by probable cause, they were unconstitutional searches. The panel rejected this argument because the defendant did not have a legitimate expectation of privacy in the limited digital data sought in the government's subpoenas, given that the subpoenas did not request any communication content from the defendant's accounts and the government did not receive any such content in response to the subpoenas.

The defendant argued that the government's search warrant affidavit failed to establish probable cause because it did not include any images of child pornography or any reasonable factual descriptions of such images. Rejecting this argument, the panel concluded that the affidavit—which described Yahoo's internal investigation and the resulting findings, as well as the information Facebook provided to the National Center for Missing and Exploited Children after searching the defendant's accounts—established a fair probability that child pornography would be found on the defendant's electronic devices. ***.

In an amended partial dissent, Judge Graber parted ways with the majority only as to the question whether, in conducting its searches of the defendant's chat messages, Yahoo was acting as an instrument or agent of the government. Judge Graber applied the two-part test set forth in *United States v. Young*, 153 F.3d 1079 (9th Cir. 1998) (per curiam) to the first prong, she wrote that the government knew of and acquiesced in Yahoo's intrusive conduct, and she rejected the suggestion that this prong would be met only if Yahoo's conduct had been illegal. As to the second prong, she wrote that Yahoo's motivation to

conduct the searches was intertwined with, and dependent on, the government's enforcement of criminal laws.

#Fourth Amendment – Warrant Required or Not

#Preservation and Spoliation

United States v. Rhine, Criminal Action No. 21-0687 (RC) (D.D.C. Jan. 24, 2023)

The defendant was charged with four misdemeanor counts related to his alleged participation in the January 6th Insurrection. He moved for, among other things, suppression of evidence derived from a geofence warrant. The warrant established a three-step process for the seizure of Google Location History data for individuals in or immediately around the Capitol over a four-and-a-half period on the date of the Insurrection. The defendant argued that the warrant lacked particularity and was overbroad. After an extensive analysis of caselaw, the district court denied the motion. Without ruling on the Government's argument that the defendant lacked a reasonable expectation in the data, the court found that the warrant was not overbroad because the geofence was limited to the "contours" of the Capitol and the timeframe "was at most co-extensive with the scope of probable cause." The court also rejected the particularity challenge, finding that three-step process did not "vest too much authority with the Government." Finally, the court held that the good faith exception would, in any event, apply.

#Fourth Amendment--Good Faith Exception

#Fourth Amendment--Particularity Requirement and/or Overbreadth

#Fourth Amendment--Warrant Required or Not

United States v. Taylor, 54 F.4th 795 (4th Cir. 2022)

The appellant moved to vacate, set aside, or correct her sentence because of ineffective assistance of counsel. She argued that her trial counsel had rendered ineffective assistance by failing to suppress information obtained from a search warrant that relied on the Government's warrantless procurement of data from her cell phone service provider. The district court denied relief. The Fourth Circuit affirmed, holding that the Government had relied in good faith on orders that had been issued under the SCA and did not request the data in the subpoenas served on the provider under the SCA. The orders were lawful at the time, predating *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

#Fourth Amendment – Warrant Required or Not

#Sixth Amendment – Assistance of Counsel

#SCA

United States v. Wiley, No. 3:21CR98 (JBA), 2022 WL 2656788 (D. Conn. July 8, 2022)

The Government moved *in limine* to admit into evidence excerpts of four rap videos as well as transcripts and images from each to show that the defendant conspired with others to sell drugs and intended to do so. The defendant opposed the motion, arguing that use of the evidence would chill his First Amendment rights and was barred by the Federal Rules of Evidence. The district court rejected the First Amendment challenge, holding that the Government's motivations for introducing the evidence were permissible under the First Amendment. Turning to Rule 403, the court allowed only those lyrics that tended to demonstrate the defendant's knowledge of the drug trade, his involvement and objectives in drug dealing, and his relationship with a

co-conspirator. The court also found that Rule 404(b) did not preclude admissibility, as the evidence would be offered to show knowledge and the like rather than the defendant's bad character. The court also held that admission would not raise Confrontation Clause issues as the videos were not "testimonial."

#Admissibility

United States v. Yung, 37 F.4th 70 (3d Cir. 2022)

The defendant applied for admission to Georgetown Law. He interviewed with an alumnus. The interview did not go well. The defendant was rejected by Georgetown and thereafter began a campaign to strike back at the alumnus that included "cyber-harassment." He was charged with cyberstalking under 18 U.S.C. Sec. 2261A(2)(B) and 2261(b). "Faced with a mountain of evidence," he unsuccessfully argued that the statutes were overbroad. The defendant then pled guilty but reserved his right to appeal, among other things, the overbreadth ruling. The Third Circuit affirmed, adopting a narrow construction of the statute to avoid a broader one that could punish speech protected by the First Amendment:

> To 'intimidate,' we hold, a defendant must put the victim in fear of death or bodily injury. And to 'harass,' he must distress the victim by threatening, intimidating, or the like. That reading limits intent to harass to 'criminal harassment, which is unprotected because it constitutes true threats or speech that is integral to proscribable criminal conduct.' ***. It also limits 'intent to intimidate' to what it 'especially' means, a form of true threats or speech integral to a crime. ***. Those narrow readings ensure that protected speech largely escapes the law's net. Thus, we can avoid the 'strong medicine' of invalidating the statute as facially overbroad. ***.

#Miscellaneous

#Social Media

#Sixth Amendment – Right of Confrontation

Matter of Use of A Cell-Site Simulator to Identify a Cellular Device in a Narcotics Trafficking Case, No. 22 M 615, 2022 WL 3645982 (N.D. Ill. Aug. 24, 2022)

The Government applied for the issuance of an order that would allow the use of a cell-site simulator to "ascertain the phone number of a Subject Phone used by an individual suspected to be engaged in narcotics trafficking." As described by the magistrate judge, the use of the simulator, "much like geofence and cell tower dumps, casts a wide net over a particular area to capture all data within that location" and raises Fourth Amendment concerns. The court granted the application because probable cause existed (assuming that such a showing was needed for use of a simulator). Moreover, limitations in the order satisfied particularity and overbreadth concerns as it was limited in geographic scope, it minimized the Government's ability to take further investigative steps, and it provided for collection to end once the suspect's phone had been identified and deletion of all other data collected. [footnote omitted].

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

<u>DECISIONS – STATE</u>

Commonwealth v. DeJesus, 489 Mass. 292, 182 N.E.3d 280 (2022)

The defendant was observed by a police officer brandishing a weapon with an extended magazine in video recordings on a social media platform. Officers then went to a multifamily dwelling that was not the defendant's home where they found the defendant and the weapon in

a basement that appeared to be where the videos had been filmed. The defendant was arrested and moved to suppress the weapon, arguing that it was obtained through an unlawful warrantless entry. The Massachusetts Supreme Judicial Court affirmed the defendant's convictions for possessing a weapon and possessing a large capacity feeding device and, in doing so, abolished that state's "separate standing requirement:"

> Article 14's separate standing requirement poses a potential constitutional dilemma, as it 'might lead to the untenable result that the Massachusetts Declaration of Rights does not protect rights guaranteed by the Federal Constitution (i.e., where a defendant has no possessory interest in the area or item searched, but does have a reasonable expectation of privacy in it). ***, Such a situation is most likely to arise in the context of electronic data. A defendant with a reasonable expectation of privacy in such data might have a difficult time asserting possession of it or presence at the time of the search. ***, 'For example, a defendant could send a text message using an encrypted messaging service, where the message subsequently was acquired from the recipient device by law enforcement. Assuming that the defendant could establish a reasonable expectation of privacy based on the use of the encryption technology employed, the defendant would have standing under the Fourth Amendment to contest the search that yielded the text message. Using the two-part analysis under art. 14, however, the defendant likely would be unable to establish standing if he or she had no possessory interest in the recipient device and was not present during the search. This discrepancy cannot stand.' ***.
>
> Because the Massachusetts Constitution may not provide less protection to defendants than the Federal Constitution, we hereby abandon the separate standing requirement and conclude that under art. 14, as under the Fourth Amendment, a defendant need show only a reasonable expectation of privacy in the place searched to contest a search or seizure. ***. [citations omitted].

The court then rejected the defendant's argument that he had a reasonable expectation of privacy:

As a preliminary matter, the defendant must assert his own reasonable expectation of privacy. As the trial judge made clear in his final jury instructions, the defendant was not charged with possessing the firearm and magazine at the time of the search, but rather when the videos were filmed. ***. And although it seems that another individual was charged in connection with the videos that resulted in the charges against the defendant, there is no evidence that the codefendant actually possessed, at the time of the search, the firearm that the defendant was charged with possessing. Nor is there any suggestion that the codefendant had a reasonable expectation of privacy in the basement. The defendant must, therefore, rely on his own reasonable expectation of privacy in the place searched.

'To establish a reasonable expectation of privacy, a defendant must prove both a subjective and an objective expectation of privacy. . . The defendant bears the burden of demonstrating that he or she personally has an expectation of privacy in the place searched, and that this expectation is reasonable . . .' ***. The only record evidence here of a connection between the defendant and the basement is that the defendant was in the basement when the videos were filmed. Thus, any subjective expectation of privacy that the defendant had in the basement was unreasonable. ***. [footnote and citations omitted].

#Fourth Amendment – Warrant Required or Not

#Miscellanous

#Reasonable Expectation of Privacy

#Social Media

Commonwealth v. Perry, 489 Mass. 436, 184 N.E.3d 745 (2022)

This is a detailed and thorough decision on the constitutional limits on warrants for CSLI which, in this matter before the Massachusetts Supreme Judicial Court, led to the production of information on over 50,000 unique telephone numbers. As summarized by the court in its decision,

"[a]s law enforcement capabilities continue to develop in the wake of advancing technology, so too must our constitutional jurisprudence. To this end, we must grapple with the constitutional implications of 'tower dumps,' a relatively novel law enforcement tool that provides investigators with the cell site location information (CSLI) for all devices that connected to specific cell towers during a particular time frame.

Here, the Commonwealth obtained search warrants for seven tower dumps, *** corresponding to the locations of six robberies and an attempted robbery that resulted in a homicide, all of which investigators believed to have been committed by the same individual. After analyzing the information contained in the tower dumps, investigators determined that the defendant had been near the scenes of two of the crimes. The defendant subsequently was charged with the robberies and the homicide, and he moved to suppress all evidence obtained from the tower dumps as the fruits of an unconstitutional search. A Superior Court judge denied the motion, and the defendant filed an application in the county court seeking leave to pursue an interlocutory appeal; the single justice reserved and reported the case to the full court.

The defendant argues that the Commonwealth's use of the tower dumps intruded upon his reasonable expectation of privacy, and therefore effectuated a search under the Federal and State Constitutions. He also contends that search warrants for tower dumps are per se unconstitutional because they necessarily lack particularity. In addition, the defendant asserts that, here, the warrants were not supported by probable cause.

We agree that the government's use of the seven tower dumps was an intrusion upon the defendant's reasonable expectation of privacy, and therefore constituted a search under art. 14 of the Massachusetts Declaration of Rights. *We do not agree, however, that warrants for tower dumps are per se unconstitutional. Accordingly, investigators may use tower dumps so long as they comply with the warrant requirements of art. 14.*

Here, the second of the two search warrants was sufficiently particular and supported by probable cause, and therefore the use of the information obtained from it does not offend the Massachusetts Declaration of Rights. The first warrant, however, was not supported by probable cause, and accordingly, any

evidence obtained as a result of it must be suppressed.' [(footnotes omitted) (emphasis added)].

The warrants in issue were described as follows:

Here, it is undisputed that the Commonwealth established probable cause to believe that the offenses described in the warrant had been committed. Accordingly, we consider whether each warrant affidavit established a substantial basis to believe that a search of the requested tower dumps would produce evidence of the crimes under investigation, or would aid in the apprehension of the perpetrator. ***. We begin with the second warrant, in which the warrant affidavit discussed all of the offenses under investigation in depth, before considering the less-detailed first warrant.

A. Second warrant. The second search warrant affidavit described several notable similarities between the offenses. Each robbery, as well as the attempted robbery, was committed against a clerk at a store, almost always a convenience store, in or around Boston, sometime during the period between dusk and dark. The perpetrator always brandished a black semiautomatic pistol, which he held in his right hand. Witnesses consistently described the perpetrator as a light-skinned Black or Hispanic male, approximately six feet, two inches tall, with a medium to thin build, dressed in a black hooded jacket, dark-colored pants, black gloves, black shoes, and a black or red mask. In addition, on two occasions, surveillance footage showed a hole or a light-colored blemish on the robber's jacket. Collectively, this evidence provided a substantial basis to believe *** that the same individual had committed all of the offenses ***.

The second warrant affidavit also described evidence indicating that a suspected coventurer had acted as a getaway driver in at least three of the offenses under investigation. The robberies took place from two to eleven miles apart, and some of the locations were not near any public transportation. On October 4, 2018, the store clerk saw the perpetrator enter the passenger's side of a dark-colored sedan, without removing his mask, before quickly departing the scene. On October 6, 2018, a surveillance camera recorded video footage of a dark-colored sedan or coupe traveling at a high rate of speed along the perpetrator's path of flight, as recorded by a separate surveillance camera. Moreover, on October 31, 2018, police canines detected the perpetrator's scent along his reported flight path, but the scent ended abruptly in a public area with

no nearby public transportation, which could have indicated that the perpetrator entered a vehicle. ***.

The search warrant affidavit also described facts suggesting some reason to believe that the defendant and a coventurer had communicated with one another from a distance, either prior to or after the commission of the offense. The detective seeking the search warrant averred that, based on his experience and training, violent crimes such as those at issue often require some level of coordination amongst coventurers. See Holley, 478 Mass. at 522 (statement that particular crime often involves coordination among codefendants by cellular telephone was considered as one factor in probable cause analysis). This coordination could have taken place while the perpetrators were apart; the robber appeared to travel some distance on foot prior to or after most of the robberies, and therefore was at least temporarily separated from the getaway driver. The evidence that the perpetrator and the coventurer communicated from a distance, when combined with the affiant's statements about the over-all ubiquity of cellular telephones, provided reasonable grounds to believe that the robber and the getaway driver had used cellular telephones to communicate. ***.

Because there was reason to believe that the perpetrator used a cellular telephone to communicate with a coventurer around the time of the offenses, there also was probable cause to believe that either the perpetrator's telephone or the coventurer's telephone would have produced telephone call CSLI that would appear in the requested tower dumps, and likely in more than one of the tower dumps. This CSLI, in turn, would enable investigators to isolate potential suspects by determining which, if any, individuals had been near the scene of two or more of the offenses. ***. Accordingly, the second warrant affidavit was supported by probable cause.

B. First warrant. The affidavit in support of the first warrant, much like the affidavit in support of the second warrant, outlined significant similarities amongst the offenses then under investigation, and therefore afforded a substantial basis to believe that the offenses had been committed by the same individual. Additionally, the affidavit demonstrated reason to believe that the perpetrator had been, at least occasionally, assisted by a coventurer.

The first warrant affidavit did not, however, set forth any particularized information that the perpetrator or the coventurer owned a cellular telephone or

communicated with one another from a distance. ***. Moreover, the first warrant affidavit did not discuss the need for coventurers to communicate when committing a robbery, nor did it point to any evidence that the perpetrator and the coventurer had been separated during the commission of the crime such that they would have had to communicate from a distance.

Thus, the only ground in the first affidavit upon which to conclude that the perpetrator had possessed or used a cellular telephone to aid in accomplishing the crimes was the affiant officer's statement that 'it is very common for a person to have a cellular telephone with them at all times.' ***. Therefore, the evidence obtained pursuant to the first warrant must be suppressed. ***. [(footnote omitted) (citations omitted)].

After rejecting a particularity challenge to the warrants, the Supreme Judicial Court placed prospective limits on tower dump warrants intended to avoid "unwarranted invasions of privacy, whether intentional or inadvertent, malicious or innocent" on "innocent and uninvolved third parties whose CSLI is revealed once an application for a search warrant is allowed." The limits were that only a judge may issue a search warrant for tower dumps and that the warrant "must include protocols for the prompt and permanent disposal of any and all data that does not fil within the object of the search following the conclusion of the prosecution." The court also declared its holding applied prospectively.

#CSLI

#Fourth Amendment – Ex Ante Conditions

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

Owner Operator Indep. Drivers Ass'n, Inc. v. New York State Dep't of Transportation, 205 A.D.3d 53, 166 N.Y.S.3d 337 (2022)

This was an appeal from the dismissal of a declaratory judgement action commenced by the plaintiff association of owners and operators of commercial motor vehicles which challenged a requirement imposed by a State agency that required members of the association to install electronic logging devices in their vehicles and to produce information from the devices during roadside safety inspections. The association argued that, among other things, the warrantless inspection of the information constituted an unreasonable search and seizure under the State constitution. The Third Department rejected the appeal, concluding, among other things:

> The crux of this appeal is that the ELD rule violates the privacy rights encompassed within article I, § 12 of the NY Constitution. That provision of the NY Constitution guarantees '[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures' ***. Warrantless searches are, as a general rule, per se unreasonable unless they fall within one of the recognized exceptions to the warrant requirement ***. One such exception is the so-called administrative search exception. Warrantless administrative searches may be upheld 'where the activity or premises sought to be inspected is subject to a long tradition of pervasive government regulation and the regulatory statute authorizing the search prescribes specific rules to govern the manner in which the search is conducted' ***.
>
> Petitioners here do not challenge the existence of an administrative search exception to the warrant requirement, but argue as a threshold matter that the exception is inapplicable to the search of a person. However, the ELD rule does not require the placement of a tracking device on a driver's person or any of his or her personal belongings; it requires installation of the ELD in the vehicle itself. Indeed, the Court of Appeals has explicitly recognized that the tracking of a vehicle and the tracking of its operator are not, for constitutional purposes, one in the same ***. 'People have a greater expectation of privacy in the location of their bodies, and the clothing and accessories that accompany their bodies, than in the location of their cars' ***. We thus conclude that, so long as its criteria are

met, the administrative search exception to the warrant requirement may properly be applied to the inspections authorized by the ELD rule. We now turn to whether those prerequisites have been satisfied here.

Petitioners have conceded that commercial trucking is a pervasively regulated industry, and there can be little dispute on that point. Federal regulation of commercial trucking extends back more than eight decades ***. The regulations applicable to commercial trucking are comprehensive, touching upon nearly every aspect of the industry. Federal regulations govern a wide range of topics, including the hours of service requirements at issue here (see 49 CFR part 395), driver qualifications (see 49 CFR part 391), mandated drug and alcohol testing (see 49 CFR part 382), preservation of records (see 49 CFR part 379), training requirements (see 49 CFR part 380), technical specifications of vehicles (see 49 CFR part 393), inspection, repair and maintenance of vehicles (see 49 CFR part 396), transportation of hazardous materials (see 49 CFR part 397), minimum levels of financial responsibility for motor carriers (see 49 CFR part 387), and much more. Indeed, the meticulous oversight of this industry even extends to such things as the minimum thickness of foam mattresses installed in sleeper cabs (see 49 CFR 393.76 [e] [2] [iii]). As Supreme Court aptly observed, 'one would be hard-pressed to find an industry more pervasively regulated than the trucking industry. Thus, like the numerous federal and state courts that have considered the issue, *** we too find that commercial trucking is a pervasively regulated industry pursuant to which an administrative search may be justified.

We further find that the regulatory scheme at issue here provides adequate assurances that the inspection of ELDs will be reasonable. '[T]he [s]tate has a vital and compelling interest in safety on the public highways' ***, and the ELD mandate serves to further that substantial government interest by ensuring compliance with hours of service requirements. ***. The factual findings made by the FMCSA in connection with its rulemaking revealed that the prior system of documenting hours of service through paper records was inadequate due to the widespread and longstanding problem of falsification of such records ***. During the public listening sessions held prior to enactment of the final rule, drivers stated that motor carriers sometimes pressured them to alter their paper records ***. The paper records are also vulnerable to human error ***. In our view, automatic recording and warrantless inspection of those records offer an eminently reasonable means of combatting this problem. [footnotes omitted) (citations omitted)].

#Fourth Amendment – Warrant Required or Not

Irwin Indus. Tool Co. v. Pifer, 478 Md. 645, 276 A.3d 533 (2022)

At issue in this wrongful death and product liability action was whether the court below had erred in finding that the plaintiff had not authenticated containers and powder within those containers that the plaintiff purchased on eBay, and having made that finding, awarded summary judgement to the defendant. The Court of Appeals reversed, concluding that there was "substantial circumstantial evidence for a reasonable juror to find by a preponderance of the evidence that the powder within in the containers" were exemplars of the product sold by the defendant that contained asbestos and led to the decedent's death.

#Admissibility

Long Lake Twp. v. Maxon, No. 349230, 2022 WL 4281509 (Mich. Ct. App. Sept. 15, 2022)

This is the latest judicial "entry" in the longstanding dispute between the parties arising out of the township's use of a drone to take photos of the Maxons' property. The Michigan Supreme Court determined that the use of the drone violated the Fourth Amendment and remanded for the Court of Appeals to address the applicability of the exclusionary rule:

> This is a civil case. The township seeks a declaratory judgment and to abate a nuisance. There are no police officers involved. Rather, the township enforces its zoning ordinances through the work of inspectors and zoning enforcement officers. The penalty that might be exacted for maintenance of a nuisance is a civil fine, but the township has sought no fine. Even if the township wanted to impose a fine, MCL 117.4q describes the fine as civil. '[P]rosecutions for violations of ordinances are in a sense criminal, but . . . such violations are not criminal cases within the meaning of the statutes and rules for review by [the Supreme] Court.' ***. The unlikelihood of any penalty being exacted, and the fact that this zoning

action is not coupled with a criminal prosecution of any sort, removes it from the realm of 'quasi-criminal' matters. ***.

Assuming that the drone search was illegal, it was performed by a private party. True, that person acted at the behest of a township official. But the exclusionary rule is intended to deter police misconduct, not that of lower-level bureaucrats who have little or no training in the Fourth Amendment. There is no likelihood that exclusion of the drone evidence in this zoning infraction matter will discourage the police from engaging in future misconduct, since the police were never involved in the first place. Rather, exclusion of the drone evidence likely will deter a township employee who works in the zoning arena from ever again resorting to a drone to gather evidence of a zoning violation. This is not the purpose of the exclusionary rule.

The cost of excluding this evidence is high. According to the record, the Maxons unsuccessfully attempted to fence in their illegal junkyard, signaling that they knew they were violating zoning rules or the settlement agreement, or both. Even without a fence, trees and vegetation make it difficult to see their property from ground level. Enforcement of the township's zoning ordinance in this situation may depend on the use of drone evidence. And even assuming some marginal deterrent value impacting township officials, the benefit of suppression of the evidence is vastly outweighed by the public's interest in enforcement of zoning regulations.

Finally, the Maxons have a powerful remedy for the alleged violation of their Fourth Amendment rights-a civil lawsuit sounding in constitutional tort. ***. In a criminal case, application of the exclusionary rule both punishes and penalizes the police. It also benefits the defendant, often by erasing the evidence needed to prosecute. A civil action for damages resulting from a constitutional violation also punishes and penalizes, achieving deterrence. We therefore respectfully disagree with our dissenting colleague that application of the exclusionary rule in this case is necessary to achieve deterrence. The social cost of excluding evidence in a case such as this would be substantial, however, as a public nuisance would potentially remain unabated and incapable of its own remedy.

The exclusionary rule is an essential tool for enforcing the meaning of the Fourth Amendment and discouraging law enforcement officers from trampling on

constitutional rights. The rule has been roundly criticized, but survives as demonstrated in the majority and dissenting opinions in *Utah v Strieff* ***. Here, the object of the state officials who allegedly violated the Maxons' rights was not to penalize the Maxons, but to abate a nuisance through the operation of equitable remedies. The proceedings are remedial, not punitive. The exclusionary rule was not intended to operate in this arena, and serves no valuable function. [citations omitted].

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

People v. Alexander, 207 A.D.3d 874, 172 N.Y.S. 3d 516, leave to appeal denied, 39 N.Y.3d 984 (2022), and leave to appeal denied sub nom. People v. Trini, 39 N.Y.3d 988 (2022)

The defendant pled guilty to rape and sexual abuse after his motion to suppress evidence derived from a warrant to search and seize data from his cell phone was denied. On appeal, the court first held that his written waiver of the right to appeal was invalid. The court then addressed the defendant's arguments on the merits:

Turning first to defendant's overbreadth argument, we begin by noting that 'warrants which authorize broad searches of both digital and non-digital locations may be constitutional, so long as probable cause supports the belief that the location to be searched – be it a drug dealer's home, an office's file cabinets, or an individual's laptop – contains extensive evidence of suspected crimes' ***. In order to establish probable cause, 'the warrant application must demonstrate that there is sufficient information to support a reasonable belief that evidence of a crime may be found in a certain place' ***. Here, the affidavit described the June 2018 video and the child victim's report and made clear that collectors of child pornography use a variety of electronic methods to share it, 'rarely, if ever, dispose of' it and 'may go to great lengths to conceal and protect' it. The affidavit further explained that such individuals 'also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless enable their sexual fantasies involving children.'

We agree with defendant's overbreadth contention only insofar as the affidavit was insufficient to establish probable cause to search defendant's cell phone and seize evidence related to all of the many crimes classified under Penal Law article 130 ***. Notwithstanding that overbreadth, probable cause existed to search and seize photographic and video evidence from defendant's cell phone related to his alleged June 2018 commission of the crime of sexual abuse in the first degree ***. Furthermore, even though the June 2018 video itself was not child pornography as that term is generally understood under the Penal Law ***, it was also reasonable for the issuing magistrate to conclude, based on the affidavit and the content of the June 2018 video, that a search of all data on defendant's cell phone would yield additional evidence of the crime of sexual abuse, along with crimes classified under Penal Law articles 235 and 263 ***. Therefore, because 'the warrant [i]s largely specific and based on probable cause' ***, we need only sever the overbroad portion of the warrant that directed a search for evidence of Penal Law article 130 crimes other than sexual abuse.

Moreover, our severance decision does not require exclusion of the May 2018 videos allegedly depicting him committing the crime of rape in the first degree because they are not 'the fruit[s] of the invalid portion of the search warrant' ***. Rather, we find that those videos were properly seized pursuant to the plain view doctrine, which authorizes law enforcement to seize an item in plain view if '(i) they are lawfully in a position to observe the item; (ii) they have lawful access to the item itself when they seize it; and (iii) the incriminating character of the item is immediately apparent ***. Here, the search of defendant's cell phone generated an extraction report that included thumbnail images of all of the photographs and videos covering a two-month period. Because the police could search defendant's cell phone pursuant to the valid part of the warrant, and, further, because the thumbnail images would have made the character of the May 2018 videos immediately apparent, County Court appropriately declined to exclude them ***.

Finally, we reject defendant's claim that the warrant was insufficiently particularized. To meet the particularity requirement, a warrant must (1) 'identify the specific offense for which the police have established probable cause,' (2) 'describe the place to be searched' and (3) 'specify the items to be seized by their relation to designated crimes' ***. Here, the warrant authorized police to search defendant's cell phone, which was already at the police station, and seize 'records and documents ... in the form of internet history, SMS, MMS, IM, Chats, Contacts,

GPS coordinates, Cell locations [and] Call logs' including '[a]ny access numbers, passcodes, swipe code patterns, passwords, personal identification numbers (PINS), logs, notes, memoranda and correspondence relating to computer, electronic and voice mail systems, Internet addresses and/or related contacts,' '[a]ny and all photographs and/or videos" and "GPS Location History.' The warrant's thorough description met the particularity requirement and left nothing to the discretion of the executing officers ***. [citations omitted].

#Fourth Amendment – Particularity Requirement and/or Overbreadth

People v. Bullard-daniel, 203 A.D.3d 1630, 163 N.Y.S.3d 726 (2022), lv. to appeal denied, 38 N.Y.3d 1069, 171 N.Y.S.3d 444 (2022)

The convicted of predatory assault and burglary after a jury trial. He argued on appeal that, among other things, the court below had erred in refusing to suppress DNA evidence "contained in numerous samples of seminal fluids and other biological material located in the apartment in which the incident occurred." In affirming the conviction, the Fourth Department held:

Defendant further contends that the court erred in permitting the People to introduce the results of an analysis of the DNA material using the STRmix DNA analysis program (STRmix program) because such testing is not generally accepted by the relevant scientific community. We reject that contention. Briefly, the People introduced evidence that biological samples were recovered from several locations at the scene of the incident and that those samples were analyzed using the STRmix program, which indicated that defendant's DNA was contained in those samples. Before trial, the People provided defendant with notice of the results of the tests and the program used to conduct them and, at defendant's request, the court ordered a Frye hearing concerning that program ***. The People introduced evidence at the hearing that the STRmix program had been the subject of numerous peer-reviewed journal articles and had been evaluated and approved by the National Institute of Standards and Technology and by the Erie County Central Police Services Forensic Laboratory before it began using the STRmix program. In addition, the People established that the STRmix program was being used by numerous forensic testing agencies and laboratories in New York, California, the United States Army, Australia, and New Zealand, and that it

had been approved by the DNA Subcommittee of the New York State Forensic Science Committee. We note that the Court of Appeals has stated with respect to the admissibility of DNA analysis programs that '[t]he [DNA] Subcommittee's approval is certainly relevant and may constitute some evidence of general acceptance at a Frye hearing' ***. Here, after reviewing the evidence introduced at the Frye hearing, we conclude that the People established that the methods employed in the STRmix program were generally accepted as reliable within the relevant scientific community at the time the DNA evidence was analyzed ***, and thus the court did not err in concluding that the results of the DNA analysis were admissible. We have considered defendant's remaining contention concerning the STRmix program, and we conclude that it lacks merit.

#Admissibility

#Miscellaneous

People v. Easley, 38 N.Y.3d 1010, 188 N.E.3d 586 (2022)(*mem.*)

The order of the Appellate Division should be affirmed. It was an abuse of discretion for the trial court to admit the results of DNA analysis conducted using the Forensic Statistical Tool without first holding a *Frye* hearing ***. Here, however, this error was harmless. The evidence of defendant's guilt was overwhelming. Video footage from a security camera inside the store was entered into evidence at trial, including footage from one camera trained on a display shelf which captured a group of men holding defendant against the shelf. The other men then scatter, leaving the video frame, at which point defendant places an item on the shelf directly in front of him before he too runs out of the frame. After approximately two minutes and fifteen seconds, during which no one approaches the shelf or the area where defendant placed the item, a police officer looks at the space on the shelf where the item was placed, walks over, and removes a gun. Rather than 'mere physical proximity,' the video shows that only defendant could have placed the item-the gun recovered minutes later-on the shelf, not 'any of the several others in the same area (dissenting op at 8). Therefore, there is no significant probability that the jury would have acquitted defendant had it not been for this error ***. As a result, we need not reach defendant's remaining arguments concerning discovery of materials related to the FST.

#Admissibility

#Discovery

#Miscellaneous

People v. Licona-Ortega, 2022 COA 27, 511 P.3d 721, cert. denied, No. 22SC252, 2022 WL 16778997 (Colo. Nov. 7, 2022)

After a fatal shooting, and being unable to locate the defendant and believing him to be armed and dangerous, the police requested the defendant's cell phone provider to ping him, as a result of which he was located, arrested, and confessed to the murder. The defendant was convicted of first degree murder. He argued on appeal, among other things, that the trial court had erred in denying his motion to suppress evidence derived from a warrantless ping of his cell phone. The appellate court affirmed the conviction:

> *** we conclude that, under the specific facts presented by this case, exigent circumstances justified the warrantless ping of Licona-Ortega's cell phone. Accordingly, the trial court correctly denied Licona-Ortega's motion to suppress.
>
> We do not hold that the police always will have an objectively reasonable belief that there is an immediate risk to public safety anytime a violent crime is committed, or that exigent circumstances will always excuse the failure to obtain a warrant in these circumstances. We hold only that under the specific facts of this case, and considering the nature of the intrusion on Licona-Ortega's rights - a ping of a cell phone as opposed to a forced entry into a residence - the police had an objectively reasonable belief that there was an immediate risk to public safety and that exigent circumstances excused the procuring of a search warrant.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

People v. McNabb, 2022 IL App (4th) 220070-U (2022)

The defendant was convicted or first degree murder and mob action arising out of a gang-related shooting death. The appealed from, among other things, the denial of his motion *in limine* to bar evidence of his Internet search history. The appellate court affirmed the convictions. As to the search history, the court held:

> We likewise conclude that the trial court did not abuse its discretion by admitting evidence that, around 3:20 a.m. on April 2, 2019, there were internet searches conducted on defendant's phone relating to a 'gt 380 pistol.' Police officers found four .380-caliber casings at the scene of the shooting on Orchard Road. It could have been pure coincidence that defendant conducted these internet searches and then found himself hours later at a party where a shooting happened. However, 'that a different, reasonable inference might be drawn from the same evidence does not make the inference which the State chose to argue improper or impossible.' ***. The evidence of defendant's search history was relevant, as it made the State's theory that defendant planned and participated in Nash's shooting 'more probable' than that theory would have been without this evidence. ***.
>
> In challenging this evidence, defendant asserts that the internet searches 'tended to mislead the jury and unfairly prejudiced them against [defendant] based on the risk that they would conflate the searches with the purchase, procurement, possession, or firing of a firearm.' Defendant's argument is unpersuasive. The jury obviously was not misled or prejudiced by defendant's internet searches, as the jury found that defendant did not personally discharge a firearm. The trial court reasonably found that the probative value of defendant's internet searches outweighed their prejudicial impact.
>
> Defendant also suggests that he may not have personally conducted these internet searches. He notes that Yates testified that on the evening of April 2, 2019, she spoke with Herbert, who was using defendant's phone. However, there was no indication at trial that anyone other than defendant had access to his phone around 3:20 a.m. on April 2, 2019. It was a reasonable inference from the evidence that defendant conducted these internet searches.

Defendant further mentions that the trial court prohibited the State from introducing evidence that Herbert possessed a .380-caliber handgun on April 11, 2019. The court ruled as it did on that issue because this firearm was excluded as having been used in Nash's shooting. The ruling as to Herbert's firearm had no relation to the evidence of defendant's internet search history. [citations omitted].

#Admissibility

People v. Reedy, 211 A.D.3d 1629 (N.Y. App. Div. 2022)

The defendant was convicted of aggravated driving while intoxicated. He argued on appeal, among other things, that there was no probable cause to stop his vehicle. The Fourth Department agreed:

*** defendant contends that the stop of defendant's vehicle was unlawful because the evidence before the suppression court is insufficient to establish that the arresting police officer had probable cause to believe that defendant had committed a traffic violation. At the suppression hearing, the officer testified that he stopped the vehicle after he visually estimated defendant's speed at 82 miles per hour in a 65 mph zone, and there was no testimony that the officer used a radar gun to establish defendant's speed. While it is well-settled that a qualified police officer's testimony that he or she visually estimated the speed of a defendant's vehicle may be sufficient to establish that a defendant exceeded the speed limit ***, here, the People failed to establish the officer's training and qualifications to support the officer's visual estimate of the speed of defendant's vehicle ***. Thus, inasmuch as the People failed to meet their burden of showing the legality of the police conduct in stopping defendant's vehicle in the first instance, we conclude that the court erred in refusing to suppress the physical evidence and defendant's statements obtained as a result of the traffic stop. Because our determination results in the suppression of all evidence supporting the crime charged, the indictment must be dismissed ***. [citations omitted].

#Admissibility

#Miscellaneous

People v. Rodriguez, 38 N.Y.3d 151, 190 N.E.3d 36 (2022)

The defendant was convicted of various offenses, including dissemination of indecent material to a minor. An intermediate appellate court reversed and remanded after concluding that the trial court had erred in admitting into evidence screenshots of text messages the defendant had sent to the victim. The Court of Appeals reversed and remanded to the lower court:

> The trial court acted within its discretion in determining that the People properly authenticated the screenshots. '[T]echnologically generated documentation [is] ordinarily admissible under standard evidentiary rubrics' and 'this type of ruling may be disturbed by this Court only when no legal foundation has been proffered or when an abuse of discretion as a matter of law is demonstrated ***. This Court recently held that for digital photographs, like traditional photographs, 'the proper foundation [may] be established through testimony that the photograph accurately represents the subject matter depicted ***. We reiterated that '[r]arely is it required that the identity and accuracy of a photograph be proved by the photographer ***, which would be the boyfriend here. Rather, 'any person having the requisite knowledge of the facts may verify" the photograph "or an expert may testify that the photograph has not been altered' ***.
>
> Here, the testimony of the victim-a participant in and witness to the conversations with defendant-sufficed to authenticate the screenshots. She testified that all of the screenshots offered by the People fairly and accurately represented text messages sent to and from defendant's phone. The boyfriend also identified the screenshots as the same ones he took from the victim's phone ***. Telephone records of the call detail information for defendant's subscriber number corroborated that defendant sent the victim numerous text messages during the relevant time period. Moreover, even if we were to credit defendant's argument that the best evidence rule applies in this context, the court did not abuse its discretion in admitting the screenshots.

#Admissibility

In re J.T., No. H048553, 2022 WL 2865856 (Cal. Ct. App. July 21, 2022), review denied (Oct. 12, 2022)

The minor here was adjudicated a delinquent and placed on probation. He challenged on appeal a gang-related probation condition. The Court of Appeal affirmed:

> We conclude that minor has not demonstrated that the challenged probation condition that he 'not knowingly post, display or transmit on social media or through his cell phone any symbols or information that [he] knows to be, or that the Probation Officer informs [him] to be, gang-related' is 'invalid in all respects and cannot have any valid application.' ***.
>
> Here, too, the probation condition *** serves the state's compelling and legitimate interest in reformation and rehabilitation. The state's legitimate interest outweighs the minimal intrusion on minor's First Amendment rights.
>
> Minor again relies on *Packingham* [*v. North Carolina,* 137 S.Ct. 1730 (2017)], but we find it distinguishable in the overbreadth context as well. *** *Packingham* involved a law that criminalized registered sex offenders' access of websites including social media. ***. This case, on the other hand, involves a probation condition that restricts, not prohibits, minor's use of social media. As the Third District Court of Appeal observed, 'many federal courts" have concluded that "the reasoning of Packingham cannot and should not be used to assess whether there may be a circumstance in which a probationer may be prohibited from utilizing social networking sites in a manner consistent with constitutional principles during the period of probation.' ***. [citations omitted].

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Probation and Supervised Release

#Social Media

People v. Wakefield, 38 N.Y.3d 367, 195 N.E.3d 19, reargument denied, 38 N.Y.3d 1121, 192 N.E.3d 1152 (2022)*, and cert. denied sub nom. Wakefield v. New York,* 143 S. Ct. 451 (2022)

The defendant in this murder case was granted leave to appeal to the Court of Appeals following his conviction, which was affirmed by the Third Department of the New York Appellate Division. An earlier compendium extensively reported in that appellate decision. The Court of Appeals, in affirming the lower appellate court, addressed the defendant's request for discovery of the source code used in DNA testing that was introduced into evidence. NB: This is a long quote but it's worthwhile reading. First, as discovery:

> Disclosure of the TrueAllele source code was not needed in order to establish at the *Frye* hearing the acceptance of the methodology by the relevant scientific community. First, defendant's initial attempt to obtain the source code was made by a July 2014 supplemental demand under the former demand-discovery provision***. Defendant was not entitled to the source code under that provision, as the source code is not a 'written report or document' made at the People's request for trial purposes and the proprietary information belonging to Cybergenetics was not in the People's possession or control ***. As we have previously explained, the former article 240 of the CPL was 'a detailed discovery regimen' and '[i]tems not enumerated in article 240 [were] not discoverable as a matter of right unless constitutionally or otherwise specially mandated' ***. Outside of his discovery demand, defendant made no further attempt to demonstrate a particularized need for the source code by motion to the court ***.
>
> Moreover, defendant's arguments as to why the source code had to be disclosed pay no heed to the empirical evidence in the validation studies of the reliability of the instrument or to the general acceptance of the methodology in the scientific community—the issue for the *Frye* hearing—and are directed more toward the foundational concern of whether the source code performed accurately and as intended ***. To the extent the testimony at the hearing reflected that the TrueAllele Casework System may generate less reliable results when analyzing more complex mixtures ***, defendant did not refine his

challenge to address the general acceptance of TrueAllele on such complex mixtures or how that hypothesis would have been applicable to the particular facts of this case. As a result, it is unclear that any such objection would have been relevant to defendant's case, where the samples consisted largely of simple (two-contributor) mixtures with the victim as a known contributor ***.

The Court of Appeals also rejected the defendant's Confrontation Clause argument:

Defendant also argues that the source code for the software is the declarant and that, in the absence of disclosure of the source code, he was deprived of his Sixth Amendment right to confront the witness against him. He maintains that the TrueAllele system involves artificial intelligence and, to some extent, draws its own inferences from the data. He asserts that Dr. Perlin's testimony was therefore that of a surrogate, merely parroting the results of the analyst.

Here, like the Lab reports on the generated DNA profiles, the report created by TrueAllele providing the likelihood ratio that defendant was a contributor to the DNA mixture profile found on the items of evidence is testimonial. The report was prepared by Cybergenetics at the request of the People for purposes of prosecutingdefendant in a pending criminal proceeding. Indeed, the DNA results were sent to TrueAllele precisely because of its 'more advanced approach to analyzing the DNA evidence'—i.e., its consideration of patterns and peaks below the stochastic threshold and ability to produce a higher match statistic. Therefore, the report satisfies our primary purpose test and was testimonial ***.

However, we reject defendant's novel argument that the source code is the declarant. Even if the TrueAllele system is programmed to have some measure of 'artificial intelligence,' the source code is not an entity that can be cross-examined. '[T]he Confrontation Clause provides two types of protections for a criminal defendant: the right physically to face those who testify against him, and the right to conduct cross-examination' ***. The essential purpose of the provision was to ensure 'a personal examination and cross-examination of the witness, in which the accused has an opportunity, not only of testing the recollection and sifting the conscience of the witness, but of compelling him to stand face to face with the jury in order that they may look at him, and judge by

his demeanor upon the stand and the manner in which he gives his testimony whether he is worthy of belief' ***.

In *Bullcoming v. New Mexico*, [564 U.S. 647 (2022)], the United States Supreme Court addressed an argument that a laboratory report could be introduced into evidence through the testimony of an analyst who did not personally perform or observe the test because the gas chromatograph machine, used to analyze the blood alcohol content of the accused's blood sample, was the 'true accuser' and the analyst who ran the test was a 'mere scrivener ***. The Court did not expressly address the concept that a machine can be a declarant, but rejected it sub silentio. Instead, the Court focused on the actions taken by the analyst who operated the machine that would be the appropriate subject of cross-examination—e.g., that the blood sample was received in an intact condition, that a particular test was performed on the sample number that corresponded to the case and that the test was performed according to protocol ***. In other words, the analyst 'certified to more than a machine-generated number' ***. Similarly, here, the instrument performs its quantitative analysis on electronic data generated by the Lab during the electrophoresis process only after the analyst sets the parameters following a human review of the data. And both the analyst who performed the electrophoresis on the DNA samples and Dr. Perlin, who fully understood the parameters and methodology of the TrueAllele software in its DNA interpretation processes, testified at trial and were subject to cross-examination.

We agree with the Appellate Division that defendant failed to preserve the separate argument that he was entitled to disclosure of the source code in order to fully cross-examine Dr. Perlin as the declarant at trial and, regardless, defendant's argument suffers from the same defect as the request for the source code for purposes of the Frye hearing. Defendant was not entitled to the source code under the former demand discovery statute. After the People refused the demand, defendant failed to make any further attempt to demonstrate a particularized need for the source code by motion to the court ***. (footnotes omitted) (citations omitted)].

#Admissibility

#Discovery

#Sixth Amendment – Right of Confrontation

People v. Watts, 2022 IL App (4th) 210590 (2022)

The defendant was found guilty of sex offenses after a jury trial. The victim, a minor, had snuck out of her home to go driving with the defendant, who had been drinking and sexually assaulted her. On appeal, the defendant argued, among other things, that the trial court had erred by admitting evidence of memes found on the defendant's phone that "indicated beliefs it was appropriate to sexually assault incapacitated women." The Appellate Court affirmed. After noting that the admissibility of memes did appear to be a novel issue, the court concluded that "the logic for treating text messages obtained from a phone like any other form of documentary evidence applies equally well to memes found on a phone." The court then reviewed the facts presented:

*** the State was able to establish the phone, taken from defendant at his arrest, actually belonged to him. Defendant provided the passcode to gain access to the phone. Indeed, no one disputed it was defendant's phone. Orr [a State witness] testified the extraction report revealed the source files for the memes were created and modified on defendant's phone with identical time stamps for each. Further, the phone revealed a text conversation between defendant and his girlfriend, Stein, which she identified and thereby authenticated as well. More importantly, the conversation with Stein happened almost contemporaneously with the 'creation' or 'modification' of the memes-whether by merely opening them to view, or otherwise. That the evidence showed the memes were created and modified while defendant exchanged text messages with Stein provided circumstantial evidence the memes belonged to him, as it would be unlikely anyone else had possession of his phone at that time. Stein also testified defendant belonged to a chat group where memes were shared. The content of the memes is also not in dispute. Thus, here, the trial court did not abuse its discretion, as there was direct and circumstantial evidence the memes were what the State claimed them to be-memes from defendant's phone. ***. At that point, after the court served its screening function, further issues of the document's use,

authorship, or the weight they should be accorded were ultimately for the jury to determine. ***. [citations omitted].

#Admissibility

I/M/O Search of Information Stored at the Premises Controlled by Google, Feb. 8, 2022, Case No. KM-2022-79 (Va. 19th Jud. Cir. Feb. 24, 2022)

The court declined to issue a geofence warrant in this matter sought by law enforcement to identify participants in a shooting. Using GPS coordinates, law enforcement created three zones at or around the scene of the shooting and proposed the use of a three-step process to identify the participants. The court found that the warrant application did not establish probable cause to search innocent patrons of the premises at the scene of the shooting. Moreover, the application was overbroad because the search zone was "geographically too large, the search time is too long, and the nature of the place to be searched is too sensitive."

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

State v. Campbell, 2022-Ohio-3626 (2022)

The defendant had been convicted of robbery. After his prison term had been completed, he was placed on probation. He executed a document that included a "consent to search" provision. While conducting a random search of the defendant's home, a probation officer found and searched his cell phone, which contained child pornography. That and other evidence led to felony charges. The defendant moved to suppress, arguing that the warrantless search of

the phone was unconstitutional, which the trial court denied. The defendant then pled and appealed. An intermediate court reversed, holding that there was no Fourth Amendment violation but that the search violated State law as there were no reasonable grounds to conduct it, as required by statute. The Ohio Supreme Court agreed that the Fourth Amendment had not been violated given the defendant's consent to search. It also agreed that Ohio law had been violated. However, the court reinstated the conviction, as the exclusionary rule applied only to constitutional, not statutory violations.

#Fourth Amendment – Warrant Required or Not

#Probation and Supervised Release

State v. Bowers, Appeal No. 2021AP1767-CR, 2022 WL 17984985 (Wis. App., 2022)

The defendant, a county sheriff's officer, was charged with misconduct in public office. He moved to suppress evidence derived from the warrantless search of his private Dropbox account, which the State accessed through his official county e-mail address by performing a password reset. The State appealed and the Court of Appeals affirmed. The State did not challenge the defendant's subjective expectation of privacy in his Dropbox account. Applying a six-factor test, the court held that the defendant had an objectively reasonable expectation of privacy. Among other things, the Court of Appeals analogized the account to "a modern-day version of a container used to store personal documents and effects." The court also rejected the applicability of the third-party doctrine because n issue came from the account and not a third party. The court did agree with the State that probable cause existed but rejected the State's argument that exigent circumstances justified the warrantless search because the State had sufficient time to obtain a warrant and had not demonstrated that there was an urgent need to search.

[NB: The facts of this decision are the same of Bowers v. County, digested above. Different issues before different courts.]

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#Preservation and Spoliation

#Reasonable Expectation of Privacy

#Third-Party Doctrin

State v. Garcia, 350 So. 3d 322 (Fla. 2022)

The Florida Supreme Court took this interlocutory appeal "to answer questions *** about whether requiring a defendant to disclose the passcode to an encrypted smartphone violates his constitutional right not to 'be compelled in any criminal case to be a witness against himself." The court held that *certiorari* jurisdiction did not lie to consider the appeal because the defendant had not suffered irreparable harm that could not be corrected on postjudgment appeal. The court also held that the order compelling disclosure did not constitute a departure from the "essential requirements of the law—another requirement for a grant of certiorari." This was because:

> The district courts of appeal have reasoned to differing conclusions about whether disclosure of a smartphone passcode is testimonial. The courts of last resort in several states have disagreed about whether the compulsion of such disclosure in circumstances like these would violate a defendant's constitutional right against self-incrimination.
>
> Nor have we or the U.S. Supreme Court conclusively addressed the scope of Fifth Amendment protections in a pretrial context such as this. Thus, had Garcia demonstrated irreparable harm and thereby required us to decide whether the order to compel departed from the essential requirements of the law, we would still reject his petition: it remains unsettled whether the Fifth

Amendment protects a criminal defendant, subject to a duly-issued warrant, from being compelled to disclose a passcode to a smartphone. We therefore cannot say on this record that the trial court departed from the essential requirements of the law.

#Fifth Amendment – Self-Incrimination

#Miscellaneous

State v. C.J.l., 471 N.J. Super. 477, 274 A.3d 611 (App. Div. 2022)

At issue here was whether a motion court erred in denying the State's motion to compel the defendant to produce the passcode to his cell phone by "overlooking critical ownership evidence and misapplying the forgone conclusion doctrine, effectively importing Fourth Amendment principles into what is a Fifth Amendment inquiry." The Appellate Division agreed and reversed:

*** the motion court also erred by importing Fourth Amendment principles into a Fifth Amendment inquiry. At the outset, the court acknowledged the warrants 'clearly gave the State' authority to search and seize 'all types of electronic things that may be capable of storing information or evidence of the alleged crime ....' But even after recognizing the validity of the search warrants, the motion court found that '[a]llowing the State to access the full contents of the phone would be [overbroad] and lead to a fishing expedition for incriminating information.'

The breadth of a search is a Fourth Amendment principle, and Andrews is clear that 'Fourth Amendment[ ] privacy protections should not factor into [the] analysis' for compelled passcode inquiries. ***. Compelling production of the passcode simply facilitates the execution of the warrant. Moreover, we note that the search warrants were inherently broad due to the nature of the underlying offense: third-degree endangering the welfare of a child. ***. Under this statute, '[a] person commits a crime of the third degree if he knowingly possesses, knowingly views, or knowingly has under his control, through any means, including the [i]nternet, less than 1,000 items depicting the sexual exploitation or abuse of a child.' Ibid. ***.

While we note that defendant did not contest the validity of the search warrants, we observe that twenty-first century communications technology provides near-limitless ways for an alleged perpetrator of child endangerment to view, possess, or control such items referenced in the statute. Given this reality, the broad scope of the warrant authorizing defendant's cell phone search is justifiable. We recognize the important privacy concerns that can be raised in circumstances such as this, however we find that valid and properly executed search warrants satisfactorily address any Fourth Amendment issues which may arise. ***. Consequently, we discern no privacy right of defendant implicated on this record.

The court then considered ownership:

The State also contends that the motion court's finding on the ownership element of the foregone conclusion test was contrary to the weight of the evidence. We again agree, and we find that the court failed to consider evidence in the record concerning ownership and operation of the phone. We have had few opportunities to interpret the foregone conclusion doctrine in connection with cell phone passcodes since [State v.] Andrews [243 N.J. 447 (2020),] was decided. Moreover, it appears that the ownership/possession element of the foregone conclusion doctrine is an issue yet to be addressed post- Andrews.

The motion court found defendant was in the "vicinity" of the phone and concluded that this was insufficient to prove defendant's ownership or operation of it. We disagree, as the court overlooked credible evidence in the record when making its findings. At the time of the search the phone was in defendant's locked bedroom; he was the sole occupant and refused to let the police in. Significantly, the email address associated with the phone's iCloud account incorporates defendant's last name and first initial. These probative facts, which suggest that defendant owned and operated the iPhone, were omitted from the motion court's analysis.

#Fourth Amendment – Warrant Required or Not

#Fifth Amendment – Self-Incrimination

State v. O, 514 P.3d 445 (N.M. Sup. 2022)

On appeal from the appellate division, the Supreme Court was petitioned to determine if the trial court abused its discretion in authenticating screenshots of messages originating from social media communications between an adult and a minor defendant, which were initiated by that minor. The court held that the authentication of social media evidence is governed by the traditional authentication standard set out in the rule governing authentication of evidence Rule 11-901 NMRA, which requires the proponent to offer evidence sufficient to support a finding that the evidence is what the proponent claims it is. In particular the messages where initiated by the minor defendant then aged 17 in the "near aftermath of the events giving rise to the underlying delinquency proceeding."

The Initial appeal sought to institute a heightened standard than otherwise contained in Rule 11-901 based on defendants contentions that social media platforms are especially susceptible to fraud and impersonation. The Supreme Court concluded that the state need only show that the messegas were more likely than not to have originated from the account that belonged to the child and that the child was more likely than not the author of those messages. To do so the state authenticated the messages through the testimony of Jeremiah Erickson as to the accuracy and his personal knowledge of the messages. The defendant objected on the grounds that it could not be established that only the child could have sent the messages. The Supreme Court explained that the authentication of evidence "goes to conditional relevency" State v. Arrendondo, 2012-NMSC-013, ¶ 9, 278 P.3d 517 and triggers a "two-step procedure; the judge initially plays a limited [but important], screening role, and the jury then makes the final decision on the question of fact," ultimately determining the

weight of the evidence" Edward J. Imwinkelried, Evidentiary Foundations § 4.01[1], at 43 (Matthew Bender 11th ed. 2020).

The Supreme Court ultimately concluded that the proponent does not need to demonstrate authorship of the evidence conclusively and that arguments contesting authorship go to the weight of the evidence, not it admissibility. The court came to this conclusion after considering that authentication challenges that one faces, such as the authorship of social media messages, are not unlike the challenges of conventionally written messages one might find in a letter or personal notebook, which could be susceptible to forgery. As such, the court was not convinced that the authentication of social media messages faced unique issues requiring a different standard. Additionally, the court considered that a heightened standard for social media authentication like one might find suggested in Griffin v. State, 419 Md. 343, 19 A.3d 415 (2011), would too often keep from the fact-finder reliable evidence based on an artificially narrow subset of authentication factors ultimately hindering the truth-seeking process.

#Admissibility

#Social Media

State v. Riley, 170 Idaho 572, 514 P.3d 982 (2022)*, reh'g denied* (Aug. 24, 2022)

At issue here was whether the trial court erred in suppressing drug-related evidence when a drug dog alerted on the defendant's vehicle while she was being cited for a trafficoffense. The trial court concluded that the police officer's "deviations from the traffic stop measurably and unlawfully extended the duration of Riley's seizure under the Fourth Amendment." The Idaho Supreme Court reversed and remanded:

Most importantly, the record is clear that the drug dog alerted a full 48 seconds before Officer Kingland completed writing Riley's traffic citation, an event that established reasonable suspicion of new unlawful activity. Thus, the 28 seconds of deviation did not actually lengthen the stop because even without the deviations, the drug dog would still have alerted 20 seconds before the citations were complete. Once the drug dog alerted, there was reasonable suspicion to extend the stop.

Based on this timeline, we cannot conclude that the two brief deviations actually extended the overall length of Riley's traffic stop. Although the conversations temporarily deviated from the original purpose of the stop, these 28-second detours did not extend the duration of the stop beyond the time when reasonable suspicion of a new crime arose. Specifically, when the drug dog alerted on the vehicle, reasonable suspicion of a drug offense arose, thereby initiating a new timeline. Neither deviation, individually or combined, prolonged the actual length of Riley's stop because the dog alerted before the traffic stop was completed regardless of whether the detours occurred. Thus, our standard under Rodriguez remains satisfied—the deviations did not 'prolong' or 'add time' to the overall duration of the traffic stop. Therefore, we reverse the district court's order granting Riley's motion to suppress.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

[NB: This decision includes a graphic depiction of the timelines of the traffic stop which I could not duplicate in this summary. For the timelines, go to file:///C:/Users/13058/Downloads/49087.pdf]

State v. Watson, 472 N.J. Super. 381, 277 A.3d 39 (App. Div. 2022)

The defendant was convicted of bank robbery and was given an extended prison sentence. He argued on appeal, among other things, that the trial court had erred in allowing a police officer to give improper lay witness testimony in "narrating a surveillance video as it was shown to the jury and to commenting on screenshot photographs."

The Appellate Division affirmed the conviction and remanded on a restitution question. As to the surveillance video testimony, the court reasoned:

> We conclude that the trial court did not abuse its discretion by allowing a police witness to narrate surveillance video as it was being played to the jury. We decline to substitute our judgment for the trial court's in determining whether the officer's narration comments were helpful to the jury in understanding what was being shown in the video. We note that the admission of surveillance video recordings at trial is becoming more common because of the proliferation of government, commercial, and residential surveillance cameras. To improve the process by which police narration testimony is scrutinized, we recommend a new practice and procedure whereby a trial court would conduct a Rule 104 hearing whenever the prosecutor intends to present narration testimony in conjunction with playing a video recording to the jury. At the in limine hearing, the court should consider and rule upon narration comments that will be permitted and those that will be foreclosed, providing clear instructions for the witness to follow. That would obviate the need for a series of spontaneous objections in the presence of the jury as well as the need to issue curative instructions when an objection is sustained. We also propose that the Committee on Model Criminal Jury Charges (Model Jury Charge Committee) consider whether it would be appropriate to draft a model instruction specifically tailored to address testimony that narrates or otherwise comments on video recordings as they are being played to the jury.

#Admissibility

Taylor v. Tolbert, 644 S.W.3d 637 (Tex. 2022)

This civil action arose out of a "highly-acrimonious family-law case." Suffice it to say that text messages and email were retrieved from an iPad and turned over to an attorney for use in the case. This led to charges that the attorney and others had violated federal and Texas wiretapping laws, pursuant to which private parties can seek civil relief

for violations of the laws. Addressing attorney immunity as a defense, the Texas Supreme Court held:

Under Texas law, attorneys are generally immune from civil liability to nonclients for actions taken within the scope of legal representation if those actions involve "the kind of conduct" attorneys engage in when discharging their professional duties to a client. In recent years, we have had several occasions to consider the scope of this common-law immunity defense. When presented with the question, we have held that the immunity inquiry focuses on the function and role the lawyer was performing, not the alleged wrongfulness, or even asserted criminality, of the lawyer's conduct. The nuance presented here is whether an exception exists for private-party civil suits asserting that a lawyer has engaged in conduct criminalized by statute.

We hold that, when conduct is prohibited by statute, the attorney-immunity defense is neither categorically inapplicable nor automatically available, even if the defense might otherwise cover the conduct at issue. In such cases, whether an attorney may claim the privilege depends on the particular statute in question. That being so, the attorney in this case is only entitled to partial immunity on civil claims alleging she violated state and federal wiretap statutes by ‘using’ and ‘disclosing’ electronic communications illegally ‘intercepted’ by her client and others. Immunity attaches to the state claims because the Texas wiretap statute does not expressly, or by necessary implication, abrogate the immunity defense, and the attorney met her burden to establish its applicability to the conduct at issue. But immunity does not attach to the federal claims because the federal wiretap statute is worded differently, and informative federal authority (sparse as it is) persuades us that federal courts would not apply Texas's common-law attorney-immunity defense to a claim under that statute. We thus affirm the court of appeals’ judgment that the attorney-immunity defense is inapplicable to the federal wiretap claims but reverse and render judgement for the attorney on the state wiretap claims. [footnotes omitted].

#Miscellaneous

DECISIONS AND OTHER "OFFICIAL" – FOREIGN

House of Lords, "Technology Rules? The Advent of New Technologies in the Justice System" (Justice and Home Affairs Comm., 1st Report of Session 2021-22: published March 30, 2022), https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf

#International

#Miscellaneous

USDOJ, "Joint Statement by the United States and the United Kingdom on Data Access Agreement" (Office of Public Affairs: July 21, 2022), (DOJ 22-784), https://www.justice.gov/opa/pr/joint-statement-united-states-and-united-kingdom-data-access-agreement#:~:text=The%20Data%20Access%20Agreement%20will%20allow%20information%20and%20evidence%20that,more%20quickly%20than%20ever%20before.

#International

USDOJ, "Landmark U.S.-UK Data Access Agreement Enters into Force" (Office of Public Affairs: Oct. 3, 2022), (DOJ 22-1051)https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force#:~:text=The%20Agreement%20between%20the%20Government,%E2%80%9D)%20entered%20into%20force%20today.

#International

USDOJ, Office of International Affairs ("OIA") Home Page, https://www.justice.gov/criminal-oia

The **Office of International Affairs (OIA)** returns fugitives to face justice, transfers sentenced persons to serve their sentences in their

home countries, and obtains essential evidence for criminal investigations and prosecutions worldwide by working with domestic partners and foreign counterparts to facilitate the cooperation necessary to enforce the law, advance public safety, and achieve justice.

#International

STATUTES, REGULATIONS, ETC. – FEDERAL

Fed. R. Crim. P. 16 amended effective December 1, 2022 to require United States district courts to set times for disclosures by the Government and defendants to make expert disclosures in writing. See an overview, see Battaglia article below. For the amendment itself, see Note of the Advisory Committee on Rules to the 2022 Amendment at https://www.law.cornell.edu/rules/frcrmp/rule_16

#Discovery

28 CFR Part 201 – Data Protection Review Court, https://www.ecfr.gov/current/title-28/chapter-I/part-201

#International

Federal Bureau of Investigation Training Document, "(U/FOUO FBI's Ability to Legally Access Secure Messaging App Content and Metadata" (Jan. 7, 2021),

#Encryption

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#SCA

Federal Defender Services Office, "San Francisco Police Are Using Driverless Cars as Mobile Surveillance Cameras' (Training Division: May

20, 2022), https://www.fd.org/news/san-francisco-police-are-using-driverless-cars-mobile-surveillance-cameras

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

Office of the Director of National Intelligence, "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities Calendar Year 2021" (Office of Civil Liberties, Privacy, and Transparency: Apr. 2022), https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2291-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2021

#Fourth Amendment – Warrant Required or Not

#International

#Reasonable Expectation of Privacy

USDHS, "Feature Article: Robot Dogs Take Another Step Towards Deployment at the Border" (Release date: Feb. 1, 2022), https://www.dhs.gov/science-and-technology/news/2022/02/01/feature-article-robot-dogs-take-another-step-towards-deployment

#Miscellaneous

USDOJ, "Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement" (Press Release Sept. 15, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement

#Miscellaneous

USDOJ, “District of Columbia Man Charged with Obstruction of Justice for Illegally Recording and Publishing Grand Jury Proceedings” (United States Attorney’s Office for District of Columbia: Nov. 17, 2022), https://www.justice.gov/usao-dc/pr/district-columbia-man-charged-obstruction-justice-illegally-recording-and-publishing

#Miscellaneous

#Social Media

USDOJ, “Further Revisions to Corporate Enforcement Policies Following Discussions with Corporate Crime Advisory Group” (Office of the Deputy Attorney General: Sept. 15, 2022), https://www.justice.gov/opa/speech/file/1535301/download

#Miscellaneous

USDOJ, “Google Enters into Stipulated Agreement to Improve Legal Process Compliance Program” (Press Release: Oct. 25, 2022), https://www.justice.gov/opa/pr/google-enters-stipulated-agreement-improve-legal-process-compliance-program

#Miscellaneous

#Preservation and Spoliation

USDOJ, "Justice Dept. Withdraws Outdated Enforcement Policy Statements" (Office of Public Affairs: Feb. 3, 2023), (DOJ 23-137) https://www.justice.gov/opa/pr/justice-department-withdraws-outdated-enforcement-policy-statements

#Miscellaneous

USDOJ, “Justice Dept. Announces Report on Digital Assets and Launces Nationwide Network” (Press Release: Sept. 16, 2022),

https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network

#Miscellaneous

USDOJ, "The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" (Office of the Attorney General: Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download

#Miscellaneous

"Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" (White House: Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

STATUTES, REGULATIONS, ETC. – STATE

Arizona House Bill 2219, signed into law July 6, 2022, ("Unlawful video recording of law enforcement activity; classification; definition"), https://www.azleg.gov/legtext/55leg/2R/laws/0376.pdf

#Miscellaneous

California Assembly Bill 2799, signed into law Sept. 30, 2022, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB2799:

Existing law permits a court to exclude evidence if its probative value is substantially outweighed by specified factors, including the probability that its

admission will create substantial danger of undue prejudice. Existing law permits a court to hear and determine the question of admissibility of evidence out of the presence or hearing of the jury.

This bill would require a court, in a criminal proceeding where a party seeks to admit as evidence a form of creative expression, to consider specified factors when balancing the probative value of that evidence against the substantial danger of undue prejudice. The bill would define "creative expression" as the expression or application of creativity or imagination in the production or arrangement of forms, sounds, words, movements, or symbols, as specified. The bill would require a court, in balancing the probative value of a creative expression against the substantial danger of undue prejudice, to first consider that the probative value of the creative expression for its literal truth is minimal unless that expression meets specified conditions. The bill would then require a court to consider that undue prejudice includes the possibility that the trier of fact will treat the creative expression as evidence of the defendant's propensity for violence or criminal disposition, as well as the possibility that the evidence will inject racial bias into the proceedings. The bill would require the court to consider, if proffered and relevant to the issues in the case, credible testimony on the genre of creative expression as to the context of the expression, research demonstrating that the introduction of a particular type of expression introduces racial bias into the proceedings, and evidence to rebut such research or testimony. The bill would require a court to determine the admissibility of a form of creative expression in a hearing outside the presence and hearing of the jury, and state on the record the court's ruling and reasoning therefor.

#Admissibility

California Senate Bill 1228, signed into law Sept. 30, 2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB1228:

Existing law requires any adult person who is arrested or charged with any felony offense to provide buccal swab samples, right thumbprints, a full palm print impression of each hand, and any blood specimens or other biological samples required for law enforcement identification analysis. Existing law requires that a DNA specimen and sample be destroyed and that a searchable database profile be expunged from that databank program if the person from whom the specimen or sample was collected has no past or present offense or pending charge that

qualifies that person for inclusion in the database and if that person submits an application, as specified, and gives the court discretion to grant or deny the application.

This bill would create procedures for reference samples of DNA from a victim to a crime or alleged crime, and to reference samples of DNA from any individual that were voluntarily provided for the purpose of exclusion, as defined. The bill would require those procedures to include, among other things, requiring that law enforcement agencies use these samples only for purposes directly related to the incident being investigated, prohibiting law enforcement agencies from comparing these samples with samples that do not relate to the incident being investigated, and prohibiting law enforcement agencies from including these samples in databases that allow the samples to be compared to or matched with profiles derived from DNA evidence obtained from crime scenes. The bill would specify that these provisions do not prevent crime laboratories from collecting, retaining, and using specified DNA profiles for comparison purposes in multiple cases. By imposing additional duties on local law enforcement agencies, this bill would impose a state-mandated local program.

Idaho Statement of Officer in support of search warrant for deaths at University of Idaho, https://int.nyt.com/data/documenttools/idaho-affidavit-redacted-3/cfe7c9947da66b8c/full.pdf

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Office of the Mayor, San Francisco, "Board of Supervisors Approves Camera Access Legislation to Better Protect Residents, Businesses, and Neighborhoods" (Sept. 21, 2022), https://sfmayor.org/article/board-supervisors-approves-camera-access-legislation-better-protect-residents-businesses-and

#Discovery Materials

#Reasonable Expectations of Privacy

San Francisco Police Training Document, https://s3.documentcloud.org/documents/21970950/av-interaction-guidelines-sfpd.pdf

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

ARTICLES

"Apple Advances User Security with Powerful New Data Protections," *Apple Update* (Dec. 7, 2022), https://www.apple.com/newsroom/2022/12/apple-advances-user-security-with-powerful-new-data-protections/#:~:text=%E2%80%9CAdvanced%20Data%20Protection%20is%20Apple's,Protection%20keeps%20most%20iCloud%20data

#Encryption

K. Basu & S. Witley, "Google—DOJ Settlement Sends Message on Handling Third-Party Data," *Bloomberg Law* (US Law Week: Oct. 27, 2022), https://www.bloomberglaw.com/bloomberglawnews/us-law-week/XC6CPND8000000?bna_news_filter=us-law-week#jcite

#Miscellaneous

#Preservation and Spoliation

A.J. Battaglia, "Changing Tide in Expert Witness Procedures in Criminal Cases." *San Diego FBA* (Nov. 6, 2022), https://www.fbasd.org/post/changes-to-criminal-rule-16#:~:text=The%20amendments%20have%20been%20approved,not%20contemplated%20at%20this%20point.

#Discovery Materials

J. Bhuiyan, “Surveillance Shift: San Francisco Pilots Program Allowing Police to Live Monitor Private Security Cameras,” *The Guardian* (Oct. 4, 2022), https://www.theguardian.com/us-news/2022/oct/04/san-francisco-police-video-surveillance

#Miscellaneous

S.J. Bloom, E. Ireland, & J. Knight, “Tips to Follow DOJ Guidance and Survive Corporate Investigations,” *Bloomberg Law* (Business & Practice: Jan. 6, 2023), https://www.bloomberglaw.com/bloomberglawnews/us-law-week/X8JL37G4000000?bna_news_filter=us-law-week#jcite

#

T. Brewster, “The FBI Forced a Suspect to Unlock Amazon’s Encrypted App Wickr with Their Face,” *Forbes* (July 19, 2022), https://www.forbes.com/sites/thomasbrewster/2022/07/19/fbi-forces-open-amazon-wickr-app-with-a-suspects-face/?sh=209ca4e1633e

#Encryption

#Fifth Amendment – Self-Incrimination

M. Burgess, “Cops Hacked Thousands of Phones. Was it Legal?” *Wired* (Jan. 4, 2023), https://www.wired.com/story/encrochat-phone-police-hacking-encryption-drugs/

#Encryption

#Fourth Amendment – Warrant Required or Not

#International

R.L. Cassin, “What are the DOJ’s ‘Other Resources’ for Evaluating Corporate Compliance Programs? *The FCPA Blog* (June 2, 2022), https://fcpablog.com/2022/06/02/what-are-the-dojs-other-resources-for-evaluating-corporate-compliance-

programs/#:~:text=The%20DOJ's%20internal%20guidance%20for,Evaluation%20of%20Corporate%20Compliance%20Programs.

#Miscellaneous

Andrew Cohen & O. Kerr, "Could Better Technology Lead to Stronger 4th Amendment Privacy Protections?" (Brennan Center for Justice: Apr. 6, 2022), https://www.brennancenter.org/our-work/analysis-opinion/could-better-technology-lead-stronger-4th-amendment-privacy-protections

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

Cooley Alert, "US-UK Data Access Agreement: Top Five Things to Know" (Sept. 27, 2022), https://www.cooley.com/news/insight/2022/2022-09-27-us-uk-data-access-agreement-top-five-things-to-know

#International

J.E. Cutler, "Saving Rape Victims' DNA to Charge Them with Crimes Now Illegal," *Bloomberg Law* (Sept. 30, 2022), https://news.bloomberglaw.com/us-law-week/saving-rape-victims-dna-to-charge-them-with-crimes-now-illegal

#Admissibility

B. Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police," *Electronic Frontier Foundation* (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

O. Darcy, “Elon Musk Claims the FBI Paid Twitter to ‘Censor Info from the Public.’ Here’s What the Twitter Files Actually Show,” *CNN* (Dec. 20, 2022), https://www.cnn.com/2022/12/20/media/elon-musk-fbi-twitter-reliable-sources/index.html

#Miscellaneous

#Social Media

R. De, *et al.,* “President Biden Signs Executive Order on U.S. Intelligence Activities to Implement EU-U.S. Data Privacy Framework” (Mayer Brown: Oct. 10, 2022), https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/president-biden-signs-executive-order-on-us-intelligence-activities-to-implement-eu-us-data-privacy-framework

#International

#Miscellaneous

S. Flynn, “All of Your Messaging App Metadata the FBI Claims It Can Obtain,” MUO (Jan. 25, 2022)
#Encryption

C. Garvie, “A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations,” *Georgetown Law Center on Privacy & Technology* (Dec. 6, 2022), www.forensicwithoutscience.org

#Miscellaneous

R. Gibbon, *et al,* “Law Enforcement in the Digital Assets Space: Department of Justice Issues Report Pursuant to White House Executive Order,” *The* Anticorruption *Blog* (Squire Patton Boggs: Sept. 26, 2022), https://www.openlegalblogarchive.org/2022/09/26/law-enforcement-

in-the-digital-assets-space-department-of-justice-issues-report-pursuant-to-white-house-executive-order/

#Miscellaneous

Aaron Gordon, "San Francisco Police Are Using Driverless Cars as Mobile Surveillance Cameras," *Vice* (May 11, 2022), https://www.vice.com/en/article/v7dw8x/san-francisco-police-are-using-driverless-cars-as-mobile-surveillance-cameras

#Miscellaneous

Reasonable Expectation of Privacy

Allison Grande, "FBI Made 3.4M Warrantless US Date Searches, Report Says," *Law360* (Apr. 29, 2022), https://www.law360.com/cybersecurity-privacy/articles/1488844/fbi-made-3-4m-warrantless-us-data-searches-report-says?nl_pk=c4b45071-6651-458d-b343-10f24120cf10&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy&utm_content=2022-05-02&read_more=1&attachments=true

#Fourth Amendment – Warrant Required or Not

#International

#Reasonable Expectation of Privacy

"Amazon Gave Ring Doorbell Videos to US Police 11 Times Without Permission," *Guardian* (July 13, 2022), https://www.theguardian.com/technology/2022/jul/13/amazon-ring-doorbell-videos-police-11-times-without-permission

#Fourth Amendment – Reasonable Expectation of Privacy

#Miscellaneous

#Reasonable Expectation of Privacy

S.M. Hall & E.M. Quattrone, "Post-*Dobbs* Abortion Enforcement: Nebraska Uses Facebook Messages as Evidence," *Commercial Litig. Update* (Epstein Becker Green: Aug. 12, 2022), https://www.natlawreview.com/article/post-dobbs-abortion-enforcement-nebraska-uses-facebook-messages-evidence

#

W.W. Hamel, *et al.,* "Part 1: Cooperation in Government Investigations and Voluntary Self-Disclosure: What to Expect After DOJ's Latest Guidance" (Venable: Oct. 13, 2022), https://www.jdsupra.com/legalnews/part-1-cooperation-in-government-1938083/

#

M. Harris, "A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet," *WIRED* (Nov. 28, 2022), https://www.wired.com/story/fbi-google-geofence-warrant-january-6/ (paywall)

#

D. Harwell, "Customs Officials Have Copied Americans' Phone Data at Massive Scale," *Washington Post* (Sept. 15, 2022), https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

T.P. Hogan, "What Are the Ethical Rules for Prosecutors Regarding the Public Release of Videos in Officer-Involved Shootings?" 37 *Crim. Justice* 16 (ABA: Spring 2022), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2022/spring/what-are-ethical-rules-

prosecutors-regarding-public-release-videos-officerinvolved-shootings-answer-less-complicated-you-think/

#Miscellaneous

Aselle Ibraimova & A. Splittgerber, "EU-US Data Transfers: A Sigh of Relief?" *Reed Smith Client Alert,* (Jan. 4, 2023), https://www.reedsmith.com/en/perspectives/2023/01/eu-us-data-transfers

#International

Jones Day Insight, "DOJ Announces Major Changes to Corporate Criminal Enforcement Policies" (Sept. 2022), https://www.jonesday.com/en/insights/2022/09/doj-announces-major-changes-to-corporate-criminal-enforcement-policies

#Miscellaneous

L.M. Martin, "From Paper to Practice: Questions to Evaluate the Real-World Impact of Your Compliance Program Under DOJ Guidelines," *JDSupra* (Dec. 5, 2022), https://www.jdsupra.com/legalnews/from-paper-to-practice-questions-to-2602585/

#Miscellaneous

C. Keene, "Reverse Keyword Searches and Crime," *Lexology* (Aug. 11, 2022), https://www.lexology.com/library/detail.aspx?g=de2f5b21-a9b1-4650-a911-31dd1f39e671

#

O.S. Kerr, "How Body-Worn Cameras Are Changing Fourth Amendment Law," *The Volokh Conspiracy* (Dec. 21, 2022), https://reason.com/volokh/2022/12/21/how-body-worn-cameras-are-changing-fourth-amendment-law/

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

O.S. Kerr, "The Ninth Circuit's Stunner in *Rosenow,* and Thoughts on the Way Forward," *The Volokh Forward* (May 13, 2022), https://reason.com/volokh/2022/05/13/the-ninth-circuits-stunner-in-rosenow-and-thoughts-on-the-way-forward/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Preservation and Spoliation

B. Krebs, "Hackers Gaining Power of Subpoena via Fake 'Emergency Data Requests," *KrebsonSecurity* (Mar. 29, 2022), https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/#:~:text=It%20involves%20compromising%20email%20accounts,matter%20of%20life%20and%20death.

#Miscellaneous

N.T. Lee & C. Chin, "Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color," *Brookings* (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

K. McCarthy, "More Evidence of the CFAA Post-Van Buren/hiQ Jurisprudential Anarchy," *Tech. & Marketing Blog* (Aug. 4, 2022),

https://blog.ericgoldman.org/archives/2022/08/more-evidence-of-the-cfaa-post-van-buren-hiq-jurisprudential-anarchy-guest-blog-post.htm

#Miscellaneous

J. Menn, "Apple Says It Will Allow iCloud Backups to be Fully Encrypted," *Washington Post* (Dec. 7, 2022), https://www.washingtonpost.com/technology/2022/12/07/icloud-apple-encryption/

#Encryption

L.H. Newman, "The Surveillance State is Primed for Criminalized Abortion," *WIRED* (May 24, 2022), https://www.wired.com/story/surveillance-police-roe-v-wade-abortion/

#Discovery

#Miscellaneous

#Reasonable Expectation of Privacy

K. Owens, *et al.,* "Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives," *USENIX* (paper presented at 31st USENIX Security Symposium), https://www.usenix.org/conference/usenixsecurity22/presentation/owens

#CSLI

#Discovery Materials

Miscellaneous

#Probation and Supervised Release

B. Penn, “Evidence Avalanche Prompts Less-Is-More Pivot by US Prosecutors,” *Bloomberg Law* (June 15, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XAT2AG000000?bna_news_filter=privacy-and-data-security#jcite (paywall)

#Discovery

#Miscellaneous

#Trial-Related

K.S. Reimann, “The 2022 DOJ Enforcement Guidance: Areas for Compliance Program Focus,” *Program on Corporate Compliance and Enforcement* (NYU School of Law: undated), https://wp.nyu.edu/compliance_enforcement/2022/10/05/the-2022-doj-enforcement-guidance-areas-for-compliance-program-focus/#:~:text=This%20note%20highlights%20program%20elements,employee%20compensation%3B%20supervision%20of%20employee

#Miscellaneous

R. Sanchez, “As Police in Idaho Faced Mounting Criticism, Investigators Worked Meticulously Behind the Scenes to nab a Suspect,” *CNN* (Jan. 8, 2023), https://www.cnn.com/2023/01/08/us/idaho-student-killings-investigation-bryan-kohberger/index.html

#Miscellaneous

#Social Media

J.F. Savarese, *et al.,* “DOJ Clarifies Its Policies for Corporate Criminal Enforcement,” *Program on Corporate Compliance and Enforcement* (NYU School of Law: undated),

https://wp.nyu.edu/compliance_enforcement/2022/09/21/doj-clarifies-and-refines-its-policies-for-corporate-criminal-enforcement/

#Miscellaneous

J. Schuppe, "Police Sweep Google Searches to Find Suspects. The Tactic is Facing Its First Legal Challenge," *NBC News* (June 30, 2022), https://www.nbcnews.com/news/us-news/police-google-reverse-keyword-searches-rcna35749

#

F. Siddiqui & J. Menn, "'Hit the Kill Switch': Uber Used Covert Tech to Thwart Government Raids," *Washington Post* (July 10, 2022), https://www.washingtonpost.com/technology/2022/07/10/uber-europe-raids-kill-switch/

#International

#Miscellaneous

Sidley Update, "Making Sense of DOJ's New Monaco Memo on Corporate Enforcement" (Sept. 21, 2022), https://www.sidley.com/en/insights/newsupdates/2022/09/making-sense-of-us-dojs-new-monaco-memo-on-corporate-enforcement#:~:text=The%20Memo%20states%20that%20a,facts%20once%20it%20identifies%20them.

#Miscellaneous

P. Stein, "How Agents Get Warrants Like the One Used at Mar-a-Lago, and What They Mean," *Washington Post* (Aug. 11, 2022), https://www.washingtonpost.com/national-security/2022/08/11/trump-warrant-explained/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Twitter Help Center, "Guidelines for Law Enforcement," (undated), https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Social Media

Variety, "Calif. Restricts Use of Rap Lyrics in Criminal Trials After Gov. Newsom Signs Bill," *NBC News* (Sept. 30, 2022), https://www.nbcnews.com/news/nbcblk/california-restricts-use-rap-lyrics-criminal-trials-gov-newsom-signs-b-rcna50271

#Admissibility

F.S. Venancio de Souza, "Roe v. Wade's Overturn: The Impact of Data Protection and Law Enforcement," *IAPP* (July 1, 2022), https://iapp.org/news/a/roe-v-wades-overturn-the-impact-on-data-protection-and-law-enforcement/

#Miscellaneous

Aruna Viswanatha & S. Gurman, "Ample Jan. 6 Evidence Helps Secure High Conviction Rate in Capitol Riot," *Wall. St. J.* (Jan. 2, 2023), https://www.wsj.com/articles/ample-jan-6-evidence-helps-secure-high-conviction-rate-in-capitol-riot-11672627806

#Discovery Materials

#Social Media

Andrea Vittorio, "New Law Buffers California Companies from Abortion Data Requests," *Bloomberg Law* (Sept. 28, 2022),

https://news.bloomberglaw.com/privacy-and-data-security/new-law-buffers-california-companies-from-abortion-data-requests

#Fourth Amendment – Warrant Required or Not

Miscellaneous

#Social Media

E. Volokh, "Hearsay Evidence Admissible in Gun Violence Restraining Order Proceeding," *The Volokh Conspiracy* (Dec. 19, 2022), https://reason.com/volokh/2022/12/19/hearsay-evidence-admissible-in-gun-violence-restraining-order-proceedings/

#Admissibility

#Sixth Amendment – Right of Confrontation