# Electronic Evidence in Criminal Investigations and Actions:

# Representative Court Decisions and Supplementary Materials

## Ronald J. Hedges, Editor

**April 2021**

Updated from 2019 and August 2020 Supplements

# Table of Contents

FOREWORD TO THE APRIL 2021 EDITION ..... v

TAGS ..... vi

ABBREVIATIONS ..... vi

DECISIONS – UNITED STATES SUPREME COURT ..... 1

*New Jersey v. Andrews,* ___ N.J. ___ (2020), *cert.* pending, No. 20-937, 2021 WL 135207 (U.S.) (filed Jan. 7, 2021) ..... 1

DECISIONS – FEDERAL ..... 1

*Alasaad v. Mayorkas,* 988 F.3d 8 (1st Cir. 2021) ..... 1

*Novak v. City of Parma,* Case No. 1:17-cv-2148 , 2021 WL 720458 (N.D. Ohio Feb. 24, 2021) ..... 2

*Robbins v. City of Des Moines,* 984 F.3d 673 (8th Cir. 2021) ..... 3

I/M/O Search of Information Stored at Premises Controlled by Google, as Further Described in Attachment A, Case No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020) ..... 4

*I/M/O Search of Information at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020) ..... 4

I/M/O Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020) ..... 6

*United States v. Beaudion,* 979 F.3d 1092 (5th Cir. 2020) ..... 7

*United States v. Birkedahl,* 973 F.3d 49 (2d Cir. 2020) ..... 7

*United States v. Bruce,* 984 F.3d 884 (9th Cir. 2021) ..... 8

*United States v. Clarke,* 979 F.3d 82 (2d Cir. 2020) ..... 8

*United States v. Fletcher,* 978 F.3d 1009 (6th Cir. 2020) ..... 10

*United States v. Miller,* 982 F.3d 412 (6th Cir. 2020) ..... 11

*United States v. Moalin,* 973 F.3d 977 (9th Cir. 2020) ..... 13

*United States v. Moore-Bush*, 982 F.3d 50 (1st Cir. 2020), panel decision vacated pending rehearing *en banc* ..... 15

*United States v. Morgan,* 1:18-CR-00108 EAW, 2020 WL 5949366, at *1 (W.D.N.Y. Oct. 8, 2020) ..... 15

*United States v. Morton,* 984 F.3d 421 (5th Cir. 2021) ..... 16

*United States v. Ryan*, No. CR-20-65, 2021 WL 795980 (E.D. La. Mar. 2, 2021) ..... 17

DECISIONS – STATE ..... 17

*Commonwealth v. Mason,* [J-44-2020] (Pa. Sup. Ct. Mar. 25, 2021) ..... 17

*Facebook, Inc. v. Superior Court,* 10 Cal. 5th 329 (2020) ..... 19

*Montague v. Maryland,* 243 A.3d 546 (Md. Ct. App. 2020) ..... 19

*People v. White,* 2021 IL App (4th) 200354 (2021) ..... 20

*Smith v. LoanMe, Inc.,* No. S260391, ___ P.3d ___, 2021 WL 1217873 (Cal. Apr. 1, 2021) ..... 21

*State v. Clemons,* 852 S.E.2d 671 (N.C. Ct. App. 2020) ..... 22

*State v. Knight,* 15 Wash. App.2d 1018 (2021) ..... 22

*State v. Pickett,* Docket No. A-4207-19T4, 2021 WL 357765, at *1-2 (N.J. Super. Ct. App. Div. Feb. 3, 2021) ..... 23

*State v. Pittman*, 367 Or 498 (2021) (en banc) ..... 24

*Swinson v. State,* S21A0396, 2021 WL 769457 (Ga. Sup. Ct. Mar. 1, 2021) ..... 27

DECISIONS – FOREIGN ..... 29

Press Release No 29/21, *H.K. v. Prokuratuur,* Case C-746/18 (Court of Justice of the European Union (Mar. 2, 2021) ..... 29

Press Release No 123/20, Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, et al.,* Court of Justice of the European Union (Oct. 6, 2020) ..... 29

STATUTES, REGULATIONS, ETC. – FEDERAL ..... 29

"(U) Clarification of information briefed during DIA's 1 December briefing on CTD," Central Intelligence Agency (unclassified: Jan. 15, 2021) ..... 29

White Paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II,* Dep't's of Commerce and Justice and Office of the Dir. of Nat'l Intelligence (Sept. 2020) ..... 29

Inspector General for Tax Administration, Letter to Senators Wyden and Warren on use of location information from commercial databases, Dep't of Treasury (Feb. 18, 2021) ..... 30

Private Industry Notification, "Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations," FBI (Mar. 10, 2021) ..... 30

FCC Enforcement Advisory, "Warning: Amateur and Personal Radio Licensees and Operators May Not Use Radio Equipment to Commit or Facilitate Criminal Acts," FCC Public Notice (released Jan. 17, 2021) ..... 30

"Privacy and Civil Liberties Oversight Board, "Report on Executive Order 12333" (Apr. 2, 2021) ..... 30

STATUTES, REGULATIONS, ETC. – STATE ..... 31

Press Release, "Governor Baker Signs Police Reform Legislation" (Mass. Governor's Press Office (Dec. 31, 2020) ..... 31

Michigan Constitution, Section 11 Searches and Seizures: ..... 31

Directive #07-21, "Guidance on the Use of Visual Aids during Closing Arguments (Criminal)," N.J. Admin. Office of the Courts (Feb. 23, 2021) ..... 31

STATUTES, REGULATIONS, ETC. – FOREIGN ..... 32

None. ..... 32

ARTICLES ..... 32

S. Airey, *et al.,* "Approaching Self-Reporting & Co-operation Standards in U.S., U.K. and French Enforcement," Paul Hastings (Dec. 15, 2020) ..... 32

L. Becker & A. Walsh, "New Criminal Rule 5(f) Firms Up Prosecutor Brady Obligations," Law360 (Jan. 27, 2021) ..... 32

K. Broda-Bahm, "Don't Assume a Civil Zoom Trial Creates Reversible Error," Persuasive Litigator (Sept. 28, 2020) ..... 32

L.J. Cameron, et al., "Courts Adopt Varying Approaches to Implementing Due Process Protections Act," *Subject to Inquiry* (McGuire Woods: Apr. 1, 2020) ..... 32

Client Alert, "SFO Investigation Powers Over Foreign Companies Limited by U.K. Supreme Court Decision," Crowell & Moring (Mar. 3, 2021) ..... 32

P. Egan, "Michigan Lawmakers Call for Change in Encrypted Police App," Detroit Free Press (Feb. 2, 2021) ..... 33

J.C. Giancario, *et al.,* "DOJ Issues Cryptocurrency Enforcement Framework, *Willkie Compliance* (Oct. 28, 2020) ..... 33

G.M. Graff, "The Furious Hunt for the MAGA Bomber," WIRED (Aug. 12, 2020) ..... 33

P. Grosdidier, "Tracking Traffic: You Think No One Knows Where You Are Driving? Think Again," Tex. Bar. J. 656 (Oct. 2020) ..... 33

D. Harwell & C. Timberg, "How America's Surveillance Networks Helped the FBI Catch the Capitol Mob," *Washington Post* (Apr. 2, 2021) ..... 33

B.M. Heberlig, B.C. Bishop & N.P. Silverman, "The Due Process Protections Act: A New Opportunity for Defense Counsel to Advocate for Broad and Meaningful Brady Orders in Criminal Cases," Steptoe (Jan. 27, 2021) ..... 34

R.J. Hedges, G. Gottehrer & J.C. Francis IV, "Artificial Intelligence and Legal Issues," Litigation (ABA: Oct 8. 2020) ..... 34

K. Hill, "How One State Managed to Actually Write Rules on Facial Recognition," N.Y. Times (posted: Feb. 27, 2021) ..... 34

C. Histed, D. Moore & D.C. Wolf, "Bot or Not? Authenticating Social Media Evidence at Trial in the Age of Internet Fakery," K&L Gates (Nov. 10, 2020) ..... 34

A. Iftimie, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," Lawfare (Apr. 19, 2021) ..... 34

L.E. Jehl, *et al.,* "Uber Criminal Complaint Raises the Stakes for Breach Response," McDermott Will & Emery (Aug. 31, 2020) ..... 35

J. Lynch & N. Sobel, "New Federal Court Rulings Find Geofence Warrants Unconstitutional," Electronic Frontier Foundation (Aug. 31, 2020) ..... 35

R. Mac, *et al.,* "Surveillance Nation," *BuzzFeed News* (Apr. 6, 2021) ..... 35

C. Metz, "Police Drones are Starting to Think for Themselves," New York Times (Dec. 5, 2020) ..... 35

C. Miller, "How Complete is "Complete" When It Comes to Digital Evidence?" Forensic Horizons (Sept. 15, 2020) ..... 35

E. Nakashima & R. Albergotti, "The FBI Wanted to Unlock the San Bernadino Shooter's iPhone, It Turned to a Little-Known Australian Firm," *Washington Post* (Apr. 14, 2021)..... 35

L.H. Newman, "How Law Enforcement Gets Around Your Smartphone's Encryption," WIRED (Jan. 15, 2021)..... 36

A. Ng, "Google is Giving Data to Police Based on Search Keywords, Court Docs Show," CNET (Oct. 8, 2020)..... 36

T.A. Pickles, "CPRA Creates New Obligations and Questions for Businesses in Connection with Criminal Investigations," GT Alert Greenberg Traurig (Nov. 12, 2020)..... 36

T. Riley, "Extremists Flocking to Encrypted Apps Could Restart Debate Over Law Enforcement Access," The Cybersecurity 202, Washington Post (Jan. 13, 2021)..... 36

J. Rubino, "WhatsApp, Signal, Telegram and iMessage: Choosing a Private Encrypted Chat App," DollarCollapse.com (Jan. 14, 2021)..... 37

J. Schuppe, "She Didn't Know Her Kidnapper. But He was Using Google Maps – and That Cracked the Case," NBC News (Dec. 29, 2020)..... 37

C. Warzel & S.A. Thompson, "They Stormed the Capitol. Their Apps Tracked Them," N.Y. Times (posted Feb. 5, 2021)..... 37

D.M. West, "Digital Footprints are Identifying Capitol Rioters," Brookings Tech Tank (Jan. 19, 2021)..... 37

Z. Whittaker, "Minneapolis Police Tapped Google to Identify George Floyd Protesters," Yahoo.com (Feb. 6, 2021)..... 38

OTHER PUBLICATIONS..... 38

M. Caldwell, *et al*., "AI-Enabled Future Crime," Crime Sci. 9 (2020)..... 38

T. Christakis & F. Terpan, "EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options," Evidence & Evidentiary Procedure eJournal (posted Feb. 3, 2021)..... 38

Press Release, Justice Dept. Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities, (USDOJ Office of Pub. Affairs: Apr. 13, 2021)..... 38

O. S. Kerr, "The Fourth Amendment Limits of Internet Content Preservation," St. Louis U. L. J., Forthcoming (posted Dec. 18, 2020)..... 38

L. Koepke, *et al.,* "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," Upturn (Oct. 2020)..... 38

C.D. Linebaugh & E.C. Liu, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Cong. Research Serv. (Mar. 17, 2021)..... 39

"Privacy Protections in State Constitutions" Nat'l Conference of State Legislatures (Nov. 6, 2020)..... 39

## FOREWORD TO THE APRIL 2021 EDITION

The first edition of *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials* was published in February of 2016. That first 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 editions followed the first and, in December of 2017, a new edition was published that incorporated everything before it into a single compilation. Thereafter, September, 2019, and August, 2020, editions were published that updated the preceding compilation. It is now April of 2021 and the time has come to publish a supplement to the prior editions.

This latest edition features links to materials, as do its predecessors. The links were last visited when it was completed in April 2021. The reader is cautioned that specific links may become stale over time. Any materials that do not have links are behind paywalls.

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 latest compilation, 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 Attorney General Healey for allowing the postings. I also want to thank Christopher Kelly, among others in the Office, for making the postings possible.

## 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

#Social Media

#Third-Party Doctrine

#Trial-Related

## ABBREVIATIONS

"Cell Site Location Information" – CSLI

"Stored Communications Act" – SCA

## DECISIONS – UNITED STATES SUPREME COURT

*New Jersey v. Andrews,* 243 N.J. 447 (2020), *cert.* pending, No. 20-937, 2021 WL 135207 (U.S.) (filed Jan. 7, 2021)

#Fifth Amendment – Self-Incrimination

## DECISIONS – FEDERAL

*Alasaad v. Mayorkas,* 988 F.3d 8 (1st Cir. 2021)

The Court of Appeals reversed the court below, which held that Customs and Border Protection policies for basic and advanced searches of electronic devices were unconstitutional. The First Circuit concluded:

> Plaintiffs bring a civil action seeking to enjoin current policies which govern searches of electronic devices at this country's borders. They argue that these border search policies violate the Fourth and First Amendments both facially and as applied. The policies each allow border agents to perform "basic" searches of electronic devices without reasonable suspicion and "advanced" searches only with reasonable suspicion. In these cross-appeals we conclude that the challenged border search policies, both on their face and as applied to the two plaintiffs who were subject to these policies, are within permissible constitutional grounds. We find no violations of either the Fourth Amendment or the First Amendment. While this court apparently is the first circuit court to address these questions in a civil action, several of our sister circuits have addressed similar questions in criminal proceedings prosecuted by the United States. We join the Eleventh Circuit in holding that advanced searches of electronic devices at the border do not require a warrant or probable cause. *** We also join the Ninth and Eleventh Circuits in holding that basic border searches of electronic devices are routine searches that may be performed without reasonable suspicion. *** We also hold the district court erroneously narrowed the scope of permissible searches at the border. [footnote and citations omitted].

#Fourth Amendment – Warrant Required or Not

#International

*Novak v. City of Parma*, Case No. 1:17-cv-2148 , 2021 WL 720458 (N.D. Ohio Feb. 24, 2021)

> Plaintiff Anthony Novak ("Novak") created a Facebook page that mimicked the official Parma Police Department's official Facebook page. He used it to post false information about the police department. As he sees it, his page was a parody and was clearly protected by the First Amendment.
>
> The Parma Police Department saw it differently. They started receiving calls from the public about Novak's Facebook page and opened an investigation. Novak portrays this investigation as a hot-headed police pursuit designed to punish him for making fun of them. But the parties' Fed. R. Civ. P. 56 materials do not support Novak's one-sided portrayal.
>
> The Sixth Circuit aptly noted that Novak's Facebook page was "either a protected parody in the great American tradition of ridiculing the government or a disruptive violation of state law. Maybe both." And, in the context of Fed. R. Civ. P. 12, the Sixth Circuit recognized, as did this Court, that Novak's portrayal of the events precluded dismissal, even when qualified immunity was considered. *Novak v. City of Parma*, 932 F.3d 421, 424 (6th Cir. July 29, 2019).
>
> But the Fed. R. Civ. P. 56 materials have revealed a different picture of the investigation and prosecution of Novak. The evidence does not show that Detective Thomas Connor and his co-defendants were acting as hot-headed police officers seeking revenge against Novak for his "parody." Rather, it shows that they sought advice from multiple sources about the legality of Novak's Facebook page and followed the proper procedures by obtaining warrants before arresting Novak, searching his property, and presenting the facts of their investigation to the County Prosecutor and grand jury.
>
> Novak's Facebook page may very well be protected by the First Amendment. At the very least, there is a genuine dispute of material fact on that issue. *Novak*, 932 F.3d at 428. But Novak mistakenly believes that his First Amendment right to post a parody on Facebook, if that is what he did, was absolute. It wasn't.
>
> Moreover, determining if Novak's Facebook page was protected by the First Amendment is not the only important issue in this case. Indeed, the Court does not even have to resolve the First Amendment issue to rule on the parties' motions for summary judgment. Because even if the content of Novak's Facebook page *was* protected, Novak's conduct in confusing the public and disrupting police operations was not. And, if

> the defendants had probable cause to arrest Novak for knowingly disrupting police operations, they are immune from civil liability. ***
>
> Nor does the fact that Novak was ultimately acquitted of the crime of disrupting police operations expose defendants to civil liability if they had probable cause to believe that Novak committed that crime. Conviction requires proof beyond a reasonable doubt, but charging someone with a crime requires only probable cause. ***
>
> Here, after considering the parties' arguments and the materials submitted pursuant to Fed. R. Civ. P. 56, the Court recognizes that there are no genuine disputes of material fact as to whether the defendants had probable cause to investigate and charge Novak with a violation of Ohio Rev. Code § 2909.04(B). For this reason, the defendants are entitled to summary judgment ***. [citations omitted].

#Miscellaneous

#Social Media

*Robbins v. City of Des Moines,* 984 F.3d 673 (8th Cir. 2021)

The plaintiff in this civil action was recording illegally parked vehicles as well as officers and civilian employees outside a police station. He was approached by an officer, who deemed his conduct suspicious. After he was detained and arrested, the plaintiff was let go but his cell phone and camera seized. He filed the action, asserting various constitutional torts. The district court granted summary judgment in favor of the defendants on the basis of qualified immunity. The district court also granted summary judgment on the plaintiff's claim that the municipal defendant failed to train its officers. The Eighth Circuit affirmed in part. The court held that the defendants were entitled to qualified immunity on the plaintiff's First Amendment retaliation claim (for his recording activity) and his Fourth Amendment claim based on the stop because of the plaintiff's suspicious behavior coupled with other facts known to the investigating officer. The appellate court also that held that the individual defendants were not entitled to qualified immunity on the plaintiff's claims that he had been arrested in fact and his property seized as the defendants had not demonstrated probable cause to engage in these warrantless acts. The Eighth Circuit affirmed the district court on the plaintiff's failure to train claim, concluding that the evidence failed to establish deliberate indifference.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

*I/M/O Search of Information Stored at Premises Controlled by Google, as Further Described in Attachment A*, Case No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020)

The Government applied for a "geofence" warrant to further its investigation into the theft and resale of certain pharmaceuticals from a commercial location. It sought to obtain cellular phone data generated within a 100 meter radius from a commercial location for three forty-five minute intervals. The "fenced" area was in a densely populated city and included, among other things, medical offices and a residential complex. The court denied the application:

> The government's warrant application suffers from overbreadth, lack of particularity, and provides no compelling reason to abandon Fourth Amendment principles in this case. *** Most importantly, the government could easily have sought a constitutionally valid search warrant if it chose. For example, if the government had constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences, the government would have solved the issues of overbreadth and lack of particularity. But, instead, the government chose to defend its position in ways that are not supported by the law and the facts and do not satisfy constitutional standards.

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

*I/M/O Search of Information at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020)

This was an amended application by the Government for a geofence warrant. As described by the court:

> The idea behind a geofence warrant is to cast a virtual net – in the form of the geofence – around a particular location for a particular time frame. The government seeks to erect three geofences. Two would be at the same location (but for different time frames), and one would be at a second location. The window for each geofence is a 45-minute time period on a particular day. As to each of these geofences, the government proposes that Google be compelled to disclose a list of unique device identifiers for devices known by Google to have traversed the respective

> geofences. The purpose of the geofences is to identify the devices known by Google to have been in the geofences during the 45-minute time frames around the Unknown Subject's appearances on surveillance video entering the two locations on three occasions. By identifying the cell phones that traversed any of the geofences, the government hopes to identify the person suspected in the theft of the pharmaceuticals, under the theory that at least one of the identified devices might be associated with the Unknown Subject.

This was the third application submitted by the Government. After the first two were denied, the Government altered the proposed search protocol to eliminate subscriber information from the application, although the Government did not describe any "methodology or protocol *** as to how Google would know which of the sought-after anonymized information identifies suspects or witnesses." The court denied the application:

> [t]he proposed warrant here seeks information on persons based on nothing other than their close proximity to the Unknown Subject at the time of the three suspect shipments, the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these *other* persons contains evidence of the offense.

The court also found that the Particularity Requirement had not been satisfied:

> This Court cannot agree that the particularity requirement is met here by virtue of the proposed geofences being narrowly tailored in a manner justified by the investigation. Attachment B to the proposed warrant, listing the items to be seized, does not identify any of the persons whose location information the government will obtain from Google. As such, the warrant puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences. A warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize ***, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information, and thus, those persons' location histories. [citation omitted].

The court concluded with these comments:

> The technological capability of law enforcement to gather information, from service providers like Google and others, continues to grow, as demonstrated here by the Amended Application. Our appeals court has

> recognized, for quite some time now, that "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive." *** In *Carpenter* and *Riley*, the Supreme Court recognized that as the use of mobile electronic devices becomes more and more ubiquitous, the privacy interests of the general public using these devices, including the privacy interest in a person's physical location at a particular point in time, warrants protection. *** Longstanding Fourth Amendment principles of probable cause and particularity govern this case, and the technological advances making possible the government's seizure of the type of personal information sought in this case must not diminish the force and scope of Fourth Amendment protections with roots in the reviled abuses of colonial times. Simply because Google can collect this information, or because the government can obtain it from Google under a "constrained" approach "justified" by the investigation's parameters, does not mean that the approach clears the hurdles of Fourth Amendment probable cause and particularity. But nor does the Court intend to suggest that geofence warrants are categorically unconstitutional. Each specific proposed application must comply with longstanding Fourth Amendment constitutional [means]. [citations omitted].

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

*I/M/O Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020)

The Government sought geofence data in connection with an arson investigation. Surveillance and investigation led the government to believe that the six locations where arson was committed were connected and that geofence data for those locations would lead to evidence of the identity of the arsonists and co-conspirators. The information sought would be limited to discrete areas and for limited time periods. The court found that probable cause had been established and that particularity satisfied given information described in the supporting affidavit as to the nature of arson offenses and the limitations on time, location, and scope.

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

*United States v. Beaudion*, 979 F.3d 1092 (5th Cir. 2020)

"This is a case about GPS searches, Fourth Amendment standing, and the Stored Communications Act." The defendant and his girlfriend were drug dealers. Law enforcement secured a warrant pursuant to the SCA for the GPS coordinates of the girlfriend's cell phone over a sixteen-hour period and used that data to intercept the car that the defendant and the girlfriend were using. Law enforcement stopped and searched the car and found narcotics. The defendant moved to suppress and entered a conditional guilty plea after his motion was denied. The Fifth Circuit affirmed. The appellate court held that the defendant lacked standing to challenge the GPS information because he did not have a reasonable expectation of privacy "in a phone and number he did not own." It also rejected the argument that *Carpenter v. United States* (*q.v.*) applied because *Carpenter* "did not address the question whether an individual maintains a legitimate expectation of privacy in a record that reveals someone else's location." The court also held that the GPS search was reasonable because it was secured consistent with the SCA.

#Reasonable Expectation of Privacy

#SCA

*United States v. Birkedahl*, 973 F.3d 49 (2d Cir. 2020)

The defendant pled guilty to possession of child pornography. On appeal he challenged, among other conditions of supervised release, one that required him to verify his compliance with the conditions through a computerized voice stress analyzer that he claimed was unreliable. The Court of appeals rejected his challenge to the condition:

> To be clear, Birkedahl's hearing-based challenge does not suggest that it was an abuse of discretion to impose the verification testing condition *itself*. He merely argues that the district court should not have included the CVSA as a means of carrying out verification testing without first holding a hearing as to its reliability. We disagree, and find that the reliability of the CVSA is a fact-specific scientific inquiry that is subject to change with the advent of new technology and the passage of time. Accordingly, whether the district court abused its discretion by including the CVSA as a permissible test without first holding a hearing is not ripe for our review.

The Second Circuit also rejected the defendant's argument that the district court should have conducted a *Daubert* hearing on the reliability of the test:

> In his briefing, Birkedahl insists that he was entitled to a *Daubert* hearing on the reliability of the CVSA test. But a *Daubert* hearing relates to the "admissibility of . . . scientific evidence at trial." *Daubert v. Merrell Dow Pharm., Inc*., 509 U.S. 579, 585 (1993) (emphasis added). Needless to say, the form of verification testing that may be required as a condition of supervised release does not turn on whether the results from such a test would be admissible as evidence at trial. *See, e.g., United States v. Johnson*, 446 F.3d 272, 278 (2d Cir. 2006) (noting that the fact that "polygraph results are inadmissible as evidence" "does not much bear on the therapeutic value of the tool" to advance sentencing goals).

#Admissibility

#Probation and Supervised Release

*United States v. Bruce*, 984 F.3d 884 (9th Cir. 2021)

The defendant, a former federal corrections officer, appealed his conviction for conspiracy and other offenses following a jury trial. He argued on appeal, among other things, that the district court had erred when it allowed into evidence a witness's identification of the defendant based on a Facebook photo. The Ninth Circuit rejected the argument and upheld the introduction of the identification at trial: "Even if the Facebook photo was suggestive, our consideration of the totality of the circumstances persuades us that the district court did not err by admitting the identification evidence."

#Admissibility

#Trial-Related

*United States v. Clarke*, 979 F.3d 82 (2d Cir. 2020)

The defendant was convicted of child pornography-related offenses following a jury trial. "The evidence showed that Clarke downloaded child pornography files to his computer, employing BitTorrent, an Internet peer-to-peer file-sharing network, and kept those files in a folder where they were available to be downloaded by other uses of the network." On appeal, the defendant challenged, among other things, the district court's denial of his motion for discovery of the software used by the Government to identify him and to download child pornography from his computer. The Second Circuit rejected his argument:

We recognize that, when a defendant's guilt is predicated on the government offering proof that a government agent downloaded files from the defendant's computer, information about the program by which the downloading was accomplished is likely to be "material to preparing the defense" and therefore subject to disclosure under Fed. R. Crim. P. 15 16(a)(1)(E)(i), so as to enable the defendant to challenge the government's proof. *** Here, the Government did provide Clarke with considerable information about the operation of the program, short of turning over the program itself and its source code. The Government's disclosures included copies of the files downloaded by the agents (as well as forensic images of the corresponding data recovered on Clarke's computer equipment), over 200 pages of data logs detailing the agents' downloads of files from his computer, a "forensic report" of the computer equipment seized from Clarke, and an in-person demonstration of how Torrential Downpour operated. This evidence showed, among other things, that the video files on the agents' computer, purportedly downloaded from the defendant's computer by use of the Torrential Downpour program, exactly matched files later recovered from Clarke's computer equipment. The Government's reason for opposing further disclosure was a substantial one—access to the material withheld would have enabled traffickers in child pornography to avoid detection by altering or avoiding the files that law enforcement was searching for. It would also enable those seeking child pornography to find those files that had been identified by the Government.

Ultimately, we need not decide whether the Government's reasons for withholding disclosure outweighed Clarke's need for it because, even assuming a violation of Clarke's entitlement to discovery, Clarke has not demonstrated that he suffered prejudice as a result. *** Clarke's argument to the district court for why disclosure of the software and its source code was necessary for his defense (in addition to the other pertinent discovery provided above) was premised on an assumption made by his expert that, because the child pornography files accessed by the government agents were located on Clarke's external hard drive, rather than his computer's hard drive, the files "would not have been publicly available on the BitTorrent network" and therefore that Clarke's computer could not have shared or transported them. *** Accordingly, Clarke argued, access to Torrential Downpour and its source code was necessary for him to show that the government agents could not have downloaded Clarke's child pornography files over the open BitTorrent network.

The Government, however, persuasively countered Loehrs's [a defense expert] assertions with evidence that the district court was entitled to

> credit. The Government's evidence showed that, unlike some other peer-to-peer programs, uTorrent prompts the user to choose "a location to save the downloaded files" before initiating a download. *** Critically, whatever location is specified by the user as the destination for the downloaded files becomes accessible to other users of the network, regardless of whether that folder is on the computer itself or on an external hard drive. Additionally, the Government submitted evidence showing that files downloaded and saved to an external hard drive by a Department of Justice investigative analyst, using the same version of uTorrent used by Clarke, were accessed by other BitTorrent users. This evidence refuted Loehrs's assumption that files saved on external hard drives were not accessible to other users of BitTorrent, and the district court reasonably concluded that Loehrs's speculation was "insufficient to create an issue as to the [Torrential Downpour] software's reliability." *** There is thus no indication, given the extensive disclosures that were made to Clarke, that he was in any way prejudiced by the district court's denial of his demand for disclosure of the program itself and its source code. *** If the initial denial was error, Clarke has failed to make any showing that he suffered harm as a result. [citations omitted].

#Discovery Materials

*United States v. Fletcher,* 978 F.3d 1009 (6th Cir. 2020)

The defendant was convicted of importuning a minor, sentenced to five years' probation, and required to register as a sex offender. The terms of his probation forbade him from contacting his victim, any other unsupervised minors, and possessing any pornography. During a routine visit, the defendant's probation officer noticed that the defendant had two phones. After the defendant was observed to be acting nervously and looking through one of the phones, the officer requested access to it as he feared the defendant was deleting its contents. The defendant said he could not recall the passcode but later unlocked the phone with a fingerprint. The officer searched through the phone and saw an image of child pornography. The officer then turned off the phone and contacted a State detective, who secured a warrant. Child pornography was found and the defendant charged in both State and federal court. In the latter, the defendant moved to suppress the evidence recovered from the phone. The district court denied the motion and the defendant was found guilty of conspiracy to produce, and production of, child pornography. On appeal, the defendant challenged the denial of the motion as well as various sentencing issues. The Sixth Circuit reversed and remanded. It used two frameworks that govern the relationship between State actors and individuals

subject to State supervision and concluded that the initial warrantless search satisfied neither because the probation officer lacked a reasonable suspicion that would have justified the warrantless search. The appellate court also rejected the applicability of the good faith exception to the exclusionary rule because the officer's conduct was deliberate and the subsequently issued warrant was based on the officer's unlawful activity.

#Fourth Amendment – Good Faith Exception

#Probation and Supervised Release

*United States v. Miller*, 982 F.3d 412 (6th Cir. 2020)

> Courts often must apply the legal rules arising from fixed constitutional rights to new technologies in an evolving world. The First Amendment's rules for speech apply to debate on the internet. *** The Second Amendment's rules for firearms apply to weapons that did not exist "at the time of the founding." *** The Supreme Court has made the same point for the rights at issue in this criminal case: The Fourth Amendment right against "unreasonable searches" and the Sixth Amendment right to confront "witnesses." *** We must consider how the established rules for these traditional rights should apply to a novel method for combatting child pornography: hash-value matching.
>
> A hash value has been described as "a sort of digital fingerprint." *** When a Google employee views a digital file and confirms that it is child pornography, Google assigns the file a hash value. It then scans Gmail for files with the same value. A "match" signals that a scanned file is a copy of the illegal file. Here, using this technology, Google learned that a Gmail account had uploaded two files with hash values matching child pornography. Google sent a report with the files and the IP address that uploaded them to the National Center for Missing and Exploited Children (NCMEC). NCMEC's systems traced the IP address to Kentucky, and a detective with a local police department connected William Miller to the Gmail account. Miller raises various constitutional challenges to his resulting child-pornography convictions.
>
> He starts with the Fourth Amendment, arguing that Google conducted an "unreasonable search" by scanning his Gmail files for hash-value matches. But the Fourth Amendment restricts government, not private, action. And while Google's hash-value matching may be new, private searches are not. A private party who searches a physical space and hands over paper files to the government has not violated the Fourth

Amendment. *** That rule covers Google's scan of virtual spaces and disclosure of digital files.

Miller next argues that the police detective conducted an "unreasonable search" when he later opened and viewed the files sent by Google. This claim implicates another settled rule: Under the private-search doctrine, the government does not conduct a Fourth Amendment search when there is a "virtual certainty" that its search will disclose *nothing more* than what a private party's earlier search has revealed. *** So we must ask whether the detective's manual search would disclose anything more than what Google's hash-value search showed. Critically, Miller does not dispute the district court's finding about a hash-value match's near-perfect accuracy: It created a "virtual certainty" that the files in the Gmail account were the known child-pornography files that a Google employee had viewed. Given this (unchallenged) reliability, *Jacobsen's* required level of certainty is met.

Miller thus asks us to depart from *Jacobsen's* idiosyncratic definition of a Fourth Amendment "search," noting that the Supreme Court recently clarified that such a "search" also occurs when the government trespasses onto property to obtain information. *** At the least, Miller says, the detective's opening of the files qualifies as a search in this "trespass-to-chattels" sense. He raises a legitimate (if debatable) point. The Supreme Court has long required the government to obtain a warrant to open sealed letters, the equivalent of modern emails. *** Yet, well before *Jacobsen*, the Court also allowed the government to rely on letters illegally taken and opened by private parties. *** And Google arguably "opened" the files and committed the "trespass" here. In the end, though, we need not resolve this debate. We find ourselves bound by *Jacobsen* no matter how this emerging line of authority would resolve things.

Miller lastly argues that the admission of NCMEC's report at trial violated his Sixth Amendment right to confront "witnesses." This right's basic rule (that a defendant must have the opportunity to cross-examine those who make testimonial statements) certainly applies to new types of witnesses, such as forensic analysts. *** But the rule's reach is nevertheless limited to statements by "witnesses"—that is, people. And NCMEC's automated systems, not a person, entered the specific information into the report that Miller challenges. The rules of evidence, not the Sixth Amendment, govern the admissibility of this computer-generated information. [citations omitted].

#Admissibility

#Fourth Amendment – Warrant Required or Not

#Sixth Amendment – Right of Confrontation

*United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020)

The defendants were convicted for sending, or conspiring to send, money to Somalia to support a foreign terrorist organization. The Ninth Circuit affirmed the convictions:

> Their appeal raises complex questions regarding the U.S. government's authority to collect bulk data about its citizens' activities under the auspices of a foreign intelligence investigation, as well as the rights of criminal defendants when the prosecution uses information derived from foreign intelligence surveillance. We conclude that the government may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act ("FISA") when it collected the telephony metadata of millions of Americans, including at least one of the defendants, but suppression is not warranted on the facts of this case. Additionally, we confirm that the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. We do not decide whether the government failed to provide any required notice in this case because the lack of such notice did not prejudice the defendants. After considering these issues and several others raised by the defendants, we affirm the convictions in all respects.

In doing so, the appellate court rejected the defendants' argument that *Carpenter v. United States* (*q.v.*) compelled reversal. It recognized that the bulk collection of "telephony metadata" from which evidence against the defendants was derived was analogous to the CSLI in *Carpenter* but concluded:

> But we do not come to rest as to whether the discontinued metadata program violated the Fourth Amendment because even if it did, suppression would not be warranted on the facts of this case. *See United States v. Ankeny*, 502 F.3d 829, 836–37 (9th Cir. 2007) (declining to decide "close" Fourth Amendment question where suppression was "not appropriate"). Having carefully reviewed the classified FISA applications and all related classified information, we are convinced that under established Fourth Amendment standards, the metadata collection, even if unconstitutional, did not taint the evidence introduced by the government at trial. *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963).

The court also addressed, among other things, notice under the Fourth Amendment:

> At a minimum, then, the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. *See Dalia*, 441 U.S. at 248; *Berger*, 388 U.S. at 60.
>
> This constitutional notice requirement applies to surveillance conducted under FISA and the FAA, which codify the requirement with respect to several types of surveillance. 50 U.S.C. §§ 1806(c), 1825(d), 1845(c), 1881e(a)(1). It also applies to surveillance conducted under other foreign intelligence authorities, including Executive Order 12,333 and the FAA's predecessor programs. Indeed, the notice requirement is of particular importance with regard to these latter, non-statutory programs precisely because these programs lack the statutory protections included in FISA. Where statutory protections are lacking, the Fourth Amendment's reasonableness requirement takes on importance as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement.
>
> We emphasize that notice is distinct from disclosure. Given the need for secrecy in the foreign intelligence context, the government is required only to inform the defendant that surveillance occurred and that the government intends to use information obtained or derived from it. Knowledge of surveillance will enable the defendant to file a motion with the district court challenging its legality. If the government avers that disclosure of information relating to the surveillance would harm national security, then the court can review the materials bearing on its legality *in camera* and *ex parte*. *See, e.g.*, 50 U.S.C. § 1806(f) (allowing *in camera, ex parte* review of the legality of electronic surveillance under FISA Subchapter I if "the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States").

#Discovery Materials

#Fourth Amendment – Notice Required or Not

#Third-Party Doctrine

#Trial-Related

*United States v. Moore-Bush*, 982 F.3d 50 (1st Cir. 2020), panel decision vacated pending rehearing *en banc*

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

*United States v. Morgan*, 1:18-CR-00108 EAW, 2020 WL 5949366, at *1 (W.D.N.Y. Oct. 8, 2020)

The defendants were indicted for a scheme to defraud financial institutions and government-sponsored entities. They moved to dismiss the indictment on the grounds that their statutory and constitutional rights to be a speedy trial were violated. The district grant granted the motion without prejudice:

> The Court recognizes at the outset that the government has mishandled discovery in this case—that fact is self-evident and cannot be reasonably disputed. It is not clear whether the government's missteps are due to insufficient resources dedicated to the case, a lack of experience or expertise, an apathetic approach to the prosecution of this case, or perhaps a combination of all of the above. However, it is clear that the government's mistakes, while negligent, do not constitute willful misconduct undertaken in bad faith.
>
> Ultimately, the government's failures to meet court-imposed deadlines prompted the Magistrate Judge to condition the exclusion of time from the speedy trial clock on the government's production of discovery by a certain deadline—and the government blew that deadline. The government "missed" and failed to process several devices seized pursuant to a search warrant executed in May 2018. As a result, the statutory speedy trial clock has expired, and the Superseding Indictment must be dismissed.
>
> However, after careful consideration, including a detailed analysis of the adequacy of the government's electronic discovery production, the Court concludes that a dismissal with prejudice is unwarranted. The Court further concludes that Defendants' constitutional rights to a speedy trial have not been violated. Accordingly, the Superseding Indictment is dismissed without prejudice.

#Discovery Materials

*United States v. Morton*, 984 F.3d 421 (5th Cir. 2021)

The defendant was stopped for speeding. After the officers smelled marijuana, the defendant consented to a search of his van, where the officers found drugs and a glass pipe. The officers also found materials that led them to believe that the defendant might be a pedophile. He was arrested for drug possession and one of the officers applied for warrants to search three cell phones found in the van. The applications for the warrants made no mention of child exploitation but, instead, purported to seek evidence of illegal drug activity based on the attesting officer's training and experience. A judge issued the warrants and sexually explicit images of children were found. Warrants were then issued to search for child pornography and many more images were found. The defendant moved to suppress the pornographic evidence. After the district court denied the motion, the defendant entered a conditional plea. On appeal, the Fifth Circuit reversed. The appellate court held that, although the officer's affidavits established probable cause to search certain information on the phones for evidence related to illegal drug possession, there was no probable cause to search images related to drug trafficking. The Fifth Circuit also rejected the applicability of the good faith exception:

> The facts here lead to the sensible conclusion that Morton was a consumer of drugs; the facts do not lead to a sensible conclusion that Morton was a drug dealer. Under these facts, reasonably well-trained officers would have been aware that searching the digital images on Morton's phone—allegedly for drug trafficking-related evidence—was unsupported by probable cause, despite the magistrate's approval. Consequently, the search here does not receive the protection of the good faith exception to the exclusionary rule.

The court also rejected the argument that the issuing magistrate's probable cause determination made suppression inappropriate:

> However, the good faith exception, applicable to the officers, does not end our analysis. As we have said, if the good faith exception does not save the search, we move to a second step: whether the magistrate who issued the warrant had a "substantial basis" for determining that probable cause to search the cellphones existed. *** While the good faith analysis focuses on what an objectively reasonable police officer would have known to be permissible, this second step focuses on the magistrate's decision. The magistrate is permitted to draw reasonable inferences from the material he receives, and his determination of probable cause is entitled to "great deference" by the reviewing court in all "doubtful or

> marginal cases." *** At the same time, "a reviewing court may properly conclude that, notwithstanding the deference that magistrates deserve, the warrant was invalid because the magistrate's probable-cause determination reflected an improper analysis." ***
>
> Here, even giving the magistrate's determination the deference due, we hold that the magistrate did not have a substantial basis for determining that probable cause existed to extend the search to the photographs on the cellphones. Even if the warrants provided probable cause to search some of the phones' "drawers" or "file cabinets," the photographs "file cabinet" could not be searched because the information in the officer's affidavits supporting a search of the cellphones only related to drug trafficking, not simple possession of drugs. There was thus no substantial basis for the magistrate's conclusion that probable cause existed to search Morton's photographs, and the search is not saved by the magistrate's authority. The search was unconstitutional, not subject to any exceptions, and the evidence must be suppressed as inadmissible.

#Fourth Amendment – Good Faith Exception

#Miscellaneous

*United States v. Ryan*, No. CR-20-65, 2021 WL 795980 (E.D. La. Mar. 2, 2021)

The defendants were indicted for crimes related to fraudulent banking activity. They sought the entry of a standing order, and proposed a model order for the court, pursuant to the Due Process Protections Act. A magistrate judge issued an order reminding the Government of its obligation to comply with the Act. The district judge affirmed on appeal: (1) Magistrate judges have authority to issue orders under the Act and (2) the order in issue, which directed the disclosure of Brady material "within a timely manner," was appropriate.

#Discovery Materials

#Miscellaneous

#Trial-Related

## DECISIONS – STATE

*Commonwealth v. Mason*, [J-44-2020] (Pa. Sup. Ct. Mar. 25, 2021)

The defendant was employed by a family as a nanny. She was charged with various offenses related to child abuse after covert video recording revealed that she was yelling at a child before forcefully putting the child into a crib and covert

audio recording suggested that the defendant might have struck the child several times. She moved to suppress the recordings as having been made in violation of the Pennsylvania Wiretap Act, which required, among other things, that a person have a justifiable expectation that an oral communication would not be intercepted. The trial court granted the motion and the intermediate appellate court affirmed as to the audio recording, concluding that the defendant had such an expectation in the family's home where she was employed, although it held that the video was admissible. The Pennsylvania Supreme Court reversed on a discretionary appeal:

> Thus, for Appellee's motion to exclude to succeed, she carried the burden of presenting evidence to establish that, under the circumstances of this case, she possessed a justifiable expectation that the oral communications, which were captured by the nanny cam in the Valle children's bedroom, would not be intercepted. Appellee failed to meet this burden. Indeed, the only evidence Appellee submitted at the suppression hearing was her brief testimony recounting her version of the conversation that took place between her and Valle regarding the lip injury suffered by one of Valle's daughters. *** Appellee's testimony is woefully insufficient to demonstrate that she had a justifiable expectation that her oral communications would not be intercepted under the circumstances presented in this case.
>
> Further, absent demonstrable circumstances to the contrary, we believe it is objectively reasonable to conclude that persons in Appellee's position do not have a justifiable expectation that their oral communications will not be subject to interception while they are in a child's bedroom. Notably, the use of recording devices in homes as a means for parents to monitor people hired to care for their children have become so commonplace that these devices are often referred to as 'nanny cams.' That is to say that the expectation that a childcare worker is going to be recorded in their employer's home is so ubiquitous in our society that we have a name for it. Indeed, as observed above, Appellee used this term throughout her motion to suppress to describe the recording device used by Valle. *** [footnote omitted].

In dissent, two Justices took issue with, among other things, the majority's assertion that a nanny could not have an objective justifiable expectation. One dissenter wrote:

> I disagree with the Majority's conclusion that *** [the defendant] lacked a justified expectation that her oral communications would not be intercepted in her employer's home. The Majority's entire analysis hinges on the correctness of a single proposition: that the use of

> recording devices to monitor child care workers is 'ubiquitous.' The implication, of course, is that nannying is an occupation in which constant surveillance is the norm, to be expected by any reasonable caregiver. The Majority offers no support for this assertion, which strikes me as quite dubious. My own instinct—admittedly no more scientific than the Majority's—is that most parents are reluctant to place their children (and homes) in the custody of people they do not trust. [footnotes omitted].

#Miscellaneous

#Reasonable Expectation of Privacy

*Facebook, Inc. v. Superior Court,* 10 Cal. 5th 329 (2020)

This matter arose out of the quashing of a criminal defense subpoena issued by the defendant, who was charged with shooting and attempted murder. The defendant alleged that he needed all the Facebook communications by the victim of the shooting to bolster a claim of self-defense and to impeach the victim. The Supreme Court directed that the order quashing the subpoena be vacated and the trial court conduct further proceedings guided by a seven-factor "framework" to determine whether good cause existed to enforce the subpoena. The Supreme Court left open the question of whether, under its business model, Facebook was an "electronic communication service" or a "remote computing service" under the SCA. The Supreme Court also declined to address Fifth and Sixth Amendment issues "until we can be confident that we are dealing with an otherwise enforceable subpoena."

#Discovery Materials

#SCA

*Montague v. Maryland,* 243 A.3d 546 (Md. Ct. App. 2020)

The defendant was convicted of murder and other crimes. While he was incarcerated and awaiting trial, the defendant composed "jailhouse rap" that detailed the victim's murder, made references to shooting "snitches," and was posted on Instagram. The trial court allowed the lyrics to be admitted into evidence at the trial over the defendant's objection. The intermediate appellate court affirmed, as did the Maryland Court of Appeals. The court held that the lyrics were relevant and admissible because they made it more probable that the defendant murdered the victim: "The rap lyrics bear a close factual and temporal nexus to the details of *** [the] murder, and the nexus is strengthened by *** [defendant's] use

of ‘snitch’ references to potentially intimidate witnesses.” The Court of Appeals also held that the defendant’s rap lyrics had “heightened probative value that is not substantially outweighed by unfair prejudice as propensity evidence of *** [his] bad character and are therefore admissible.”

#Admissibility

*People v. White*, 2021 IL App (4th) 200354 (2021)

The defendant was convicted in a bench trial of sexual exploitation of a minor. The defendant, then a coach on the minor student’s track team, sent him “somewhat risqué photos” of herself via Snapchat. The defendant was charged under a statute that criminalized committing an act of exposure in the “virtual presence” of the minor. The Illinois Appellate Court reversed, having concluded that the images did not meet the statutory description of that presence:

> ‘Virtual presence’ means that software, such as webcam video software, creates an ‘environment’ in which the child is virtually in the defendant’s presence. *** (When used with reference to computers, ‘environment’ means the current state of the computer, determined by the combination of hardware and software programs that are running.) In this artificial environment, the child can ‘view [the defendant’s] acts’ almost if the child were there, with the defendant. *** By the virtual-presence provisions ***, the legislature has in mind a computer artifice that apes physical presence: a webcam video or something like it. To meet the description of ‘‘[v]irtual presence,’’ the software has to ‘create[ ]’ a you-could-be-there ‘environment. ***
>
> The still images that defendant texted to [the minor] W.B. did not create an ‘environment’ of virtual presence in any meaningful sense of the term. *** They were merely the digital equivalents of Polaroids, only more ephemeral. They were not calculated to create the illusion of physical presence.
>
> When someone takes out a still photograph of family members from a wallet and proudly shows it to someone, the receiver of the photograph does not feel as if he or she has been transported into a presence-simulating environment. The receiver of the still image is not moved to remark, ‘It’s almost as if I’m there, with them.’
>
> Snapchat did not create the illusory environment of presence that the legislature had in mind by its use of the term ‘virtual presence.’ Unlike Zoom, for instance, which is the video communication app that we used

for oral arguments in this case, the Snapchat app that defendant and W.B. used was not a stand-in for physical presence.

We acknowledge that, by ‘‘[w]ebcam,’’ the legislature meant ‘a video capturing device connected to a computer or computer network that is designed to take *digital photographs* or live or recorded video which allows for the live transmission to an end user over the Internet.’ (Emphasis added.) *** But that is not the same as saying that digital photographs necessarily create an ‘environment’ that apes physical presence. The definition of ‘’[v]irtual presence’’ requires the creation of such an “environment.” ***

#Miscellaneous

#Trial-Related

*Smith v. LoanMe, Inc.*, No. S260391, ___ P.3d ___, 2021 WL 1217873 (Cal. Apr. 1, 2021)

Under Penal Code section 632.7, subdivision (a) (hereinafter section 632.7(a)), it is a crime when a person ‘without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between’ a cellular or cordless telephone and another telephone. A violation of section 632.7 also can be pursued civilly and lead to the assessment of damages and other appropriate relief. The issue presented in this case is whether section 632.7 applies to the parties to a communication, prohibiting them from recording a covered communication without the consent of all participants, or whether the section is concerned only with recording by persons other than parties (sometimes hereinafter referred to as ‘nonparties’ to the communication), such as an individual who covertly intercepts a phone call and eavesdrops upon it.

The Court of Appeal concluded that section 632.7 applies only to nonparties and does not forbid a party to a phone call transmitted to or from a cellular or cordless telephone from recording the conversation without the consent of the other party or parties. We reach a contrary conclusion and hold that section 632.7 applies to parties as well as nonparties. This interpretation reflects the most sensible reading of the statutory text, is consistent with the relevant legislative history, and advances the Legislature’s apparent intent by protecting privacy in covered communications to a greater degree than the Court of Appeal’s construction would. *** [footnote omitted].

#Miscellaneous

#Reasonable Expectation of Privacy

*State v. Clemons,* 852 S.E.2d 671 (N.C. Ct. App. 2020)

> Before screenshots of an online written statement on social media can be admitted into evidence they must be authenticated as both a photograph and a written statement. To authenticate evidence in this manner, there must be circumstantial or direct evidence sufficient to conclude a screenshot accurately represents the content on the website it is claimed to come from and to conclude the written statement was made by who is claimed to have written it. Here, screenshots of comments on Facebook posts, made by an account not in Defendant's name, were properly authenticated because there was sufficient circumstantial evidence to show the screenshots of the Facebook comments in fact depicted the Facebook posts and comments and to show the Facebook comments were made by Defendant. We hold there was no error.

The screeenshots in issue were authenticated as photographs through the testimony of a woman who had secured a protective order against the defendant and who took the screenshots. They were authenticated as the defendant's written statements, although not posted in his name, through circumstantial evidence that the defendant had access to the woman's Facebook account and were made in the same timeframe as calls made to her by the defendant.

#Admissibility

*State v. Knight,* 15 Wash. App.2d 1018 (2021)

The defendant was convicted for possession of depictions of a minor engaged in sexually explicit conduct. He argued on appeal that law enforcement had conducted an unlawful warrantless search of Dropbox files received from the National Center for Missing and Exploited Children (NCMEC). The Court of Appeals affirmed his conviction. The defendant had used Dropbox to store the depictions and Dropbox reported those to the NCMEC after it had determined that the depictions were apparent child pornography. The defendant did not have a reasonable expectation of privacy in his Dropbox account because he shared links to it through a social media platform. Thus, law enforcement did not need a warrant to review the files it received from the NCMEC. Moreover, Dropbox was a private actor not subject to the Fourth Amendment. Its search of the files destroyed any reasonable expectation of privacy and, inasmuch as the NCMEC's review of

what Dropbox had sent it did not expand the scope of Dropbox's search, the private search doctrine governed. The Court of Appeals then held that the silver platter doctrine applied to the disclosure of the files to law enforcement.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Social Media

*State v. Pickett*, Docket No. A-4207-19T4, 2021 WL 357765, at *1-2 (N.J. Super. Ct. App. Div. Feb. 3, 2021)

> In this case of first impression addressing the proliferation of forensic evidentiary technology in criminal prosecutions, we must determine whether defendant is entitled to trade secrets of a private company for the sole purpose of challenging at a *Frye* hearing the reliability of the science underlying novel DNA analysis software and expert testimony. At the hearing, the State produced an expert who relied on his company's complex probabilistic genotyping software program to testify that defendant's DNA was present, thereby connecting defendant to a murder and other crimes. Before cross-examination of the expert, the judge denied defendant access to the trade secrets, which include the software's source code and related documentation.
>
> This is the first appeal in New Jersey addressing the science underlying the proffered testimony by the State's expert, who designed, utilized, and relied upon TrueAllele, the program at issue. TrueAllele is technology not yet used or tested in New Jersey; it is designed to address intricate interpretational challenges of testing low levels or complex mixtures of DNA. TrueAllele's computer software utilizes and implements an elaborate mathematical model to estimate the statistical probability that a particular individual's DNA is consistent with data from a given sample, as compared with genetic material from another, unrelated individual from the broader relevant population. For this reason, TrueAllele, and other probabilistic genotyping software, marks a profound shift in DNA forensics.
>
> TrueAllele's software integrates multiple scientific disciplines. At issue here—in determining the reliability of TrueAllele—is whether defendant is entitled to the trade secrets to cross-examine the State's expert at the *Frye* hearing to challenge whether his testimony has gained general acceptance within the computer science community, which is one of the disciplines. The defense expert's access to the proprietary information is directly relevant to that question and would allow that expert to

> independently test whether the evidentiary software operates as intended. Without that opportunity, defendant is relegated to blindly accepting the company's assertions as to its reliability. And importantly, the judge would be unable to reach an informed reliability determination at the *Frye* hearing as part of his gatekeeping function.
>
> Hiding the source code is not the answer. The solution is producing it under a protective order. Doing so safeguards the company's intellectual property rights and defendant's constitutional liberty interest alike. Intellectual property law aims to prevent business competitors from stealing confidential commercial information in the marketplace; it was never meant to justify concealing relevant information from parties to a criminal prosecution in the context of a *Frye* hearing.
>
> ***
>
> We hold that if the State chooses to utilize an expert who relies on novel probabilistic genotyping software to render DNA testimony, then defendant is entitled to access, under an appropriate protective order, to the software's source code and supporting software development and related documentation—including that pertaining to testing, design, bug reporting, change logs, and program requirements—to challenge the reliability of the software and science underlying that expert's testimony at a *Frye* hearing, provided defendant first satisfies the burden of demonstrating a particularized need for such discovery. To analyze whether that burden has been met, a trial judge should consider: (1) whether there is a rational basis for ordering a party to attempt to produce the information sought, including the extent to which proffered expert testimony supports the claim for disclosure; (2) the specificity of the information sought; (3) the available means of safeguarding the company's intellectual property, such as issuance of a protective order; and (4) any other relevant factors unique to the facts of the case. Defendant demonstrated particularized need and satisfied his burden. [footnote omitted].

#Discovery Materials

*State v. Pittman*, 367 Or 498 (2021) (en banc)

The defendant crashed her vehicle into a tree, injuring both herself and passengers. She was transported to a hospital, where staff discovered cash, a pipe, and a baggie containing a white substance. These were turned over to police officers, who suspected that the substance was methamphetamine. An officer observed a cell phone in the defendant's purse while at the hospital and secured a warrant to seize

and search it. The phone was passcode-protected so a second warrant was secured to compel the defendant to unlock the phone. She refused and the State moved to compel her to do so. The trial court ordered the defendant to unlock the phone. She did not, was held in contempt, and sentenced to 30 days' incarceration. Defendant appealed the contempt, arguing that unlocking the phone would violate her rights under the Fifth Amendment and its Oregon counterpart and that the State should be required to demonstrate that it already knew the incriminating information the phone contained. The Oregon Supreme Court first decided that the order would compel a "testimonial" act:

> We can, of course, adopt a different view in construing Article I, section 12, and hold that it is the use of the mind to assist the state that makes an act testimonial. But, to date, our decisions have been consistent with the analysis of the United States Supreme Court. In *State v. Fisher*, 242 Or 419, 422, 410 P2d 216 (1966), for example, we held that requiring a handwriting exemplar does not violate the privilege against self-incrimination. Like the act of signing a bank form, providing a handwriting exemplar requires the use of the mind, but, like the Court in *Doe II*, we did not conclude that that mental effort made that act testimonial. And in *Fish*, we, again like the Court in *Doe II*, explained the testimonial significance of conduct as stemming from what it "communicates" about a person's "beliefs, knowledge, or state of mind." *Fish*, 321 Or at 56. Today we affirm that articulation and, like most other state courts that have considered the issue, decline to hold that an act is testimonial whenever its performance requires an individual to use his or her mental faculties. The information that an act communicates, and not the uncommunicated use of the mind, is what makes an act testimonial.
>
> For the reasons given, we reject defendant's broad argument that the act of unlocking the phone would provide testimonial evidence even if it did not communicate defendant's thoughts, beliefs, knowledge, or state of mind. We return to defendant's primary argument, from the United States Supreme Court's decision in *Fisher* and this court's decision in *Fish*, that the act of unlocking the phone was protected by Article I, section 12, because it would communicate that very information.
>
> The first step in that analysis is to determine the facts, if any, that the compelled act would communicate. As *Fisher*, *Hubbell*, and *Doe II* illustrate, that depends on the order that was given. In *Fisher* the taxpayers were ordered to produce specified listed documents. Doing so, the Court held, would communicate that the documents existed, that the taxpayers had access to them, and that the taxpayers believed "that the papers are those described in the subpoena." *Fisher*, 425 US at 410. In

*Hubbell* the defendant was ordered to produce documents that fell within certain broadly described categories. 530 US at 42. Doing so would communicate not only that the documents existed, but that they fell into the described categories. In *Doe II*, the defendant was ordered to sign bank consent forms. 487 US at 203. Doing so, the Court held, would not communicate facts of any sort.

Here, defendant was ordered to unlock the phone using a passcode. Thus, as the state acknowledges, defendant's performance of that act would communicate that she knew the passcode. If the court had ordered defendant to do something different, what would be communicated by compliance with the order may have been different as well. For example, had the phone been one that could be unlocked by placing a finger on the phone, and had the court ordered defendant to place her finger on the phone, then, by performing that act, defendant would communicate only that she knew how to move her finger, not that she knew how to unlock the phone. If, however, the court had ordered defendant to unlock the phone, without specifying the means she should use to do so, then any act that she performed that served to unlock the phone would communicate her knowledge—that she knew how to comply with the court's order and how to access the phone's contents. Here, as the state acknowledges, the court's order was of that ilk. It required defendant to unlock the phone using a passcode, and compliance with that order would communicate that defendant knew that passcode. We conclude that the act of unlocking the phone was an act that would provide incriminating testimonial evidence. [citations omitted].

The Court then focused on the Oregon Constitution:

We recognize that, if a defendant complies with an order to unlock a phone, that act will reveal the contents of the phone providing the state with evidence that it could not otherwise obtain. *But, as we have explained, once the state has obtained a valid warrant to search a phone, a defendant does not have a legal right to keep the contents of the phone from the state. It is only the testimonial aspects of the act of unlocking the phone, and not the practical result of unlocking the phone, that have constitutional significance under Article I, section 12.* The testimonial aspects of the act have constitutional significance, which we must address; the access that the act provides does not.

We also recognize that, in Oregon, an individual's right against self-incrimination must be protected, no matter how weighty the state's contrary interests may be. But Article I, section 12, permits a substitute for that right that is protective to "the same extent in scope and effect," *Soriano*, 68 Or App at 663, as the right against self-incrimination and, in

> the circumstances that this case presents, we can craft a rule that meets those terms. There may come a day in which the state can conduct, pursuant to warrant, an appropriately limited search of a cell without compelling a defendant's assistance to unlock it. *See State v. Brown*, 301 Or 268, 278 n 6, 721 P2d 1357 (1986) ("In this modern day of electronics and computers, we foresee a time in the near future when the warrant requirement of the state and federal constitutions can be fulfilled virtually without exception."); *State v. Kurokawa-Lasciak*, 351 Or 179, 188-89, 263 P3d 336 (2011) (noting that the majority in *Brown* had suggested that its decision was "a temporary accommodation subject to change in the near future when technology would permit neutral magistrates to" issue warrants "more expeditiously"). *But, today, faced with the circumstances and law as they presently exist, we construe Article I, section 12, to permit an order compelling a defendant to unlock a cell phone so long as the state (1) has a valid warrant authorizing it to seize and search the phone; (2) already knows the information that the act of unlocking the phone, by itself, would communicate; and (3) is prohibited from using defendant's act against defendant, except to obtain access to the contents of the phone.* [emphasis added].

Addressing burden of proof, the Supreme Court held that, "to obtain an order requiring a defendant to unlock a cell phone, the state must prove, beyond a reasonable doubt, that it already knows the information that that act would communicate." The court ended by ordering a remand for further proceedings:

> In this case, we have concluded that the trial court did not conduct the necessary factfinding to determine whether the state had established that defendant knew the passcode to the phone and could access it contents, and, therefore, that the second requirement that would have permitted the court to order defendant to unlock the phone was not met. The third requirement—that the court's order expressly prohibit the state from using the compelled act against defendant—also was absent, although we recognize that the state apparently did not dispute that such a requirement would be appropriate. We conclude that the trial court's order compelling defendant to unlock the cell phone violated Article I, section 12. [footnote omitted].

#Fifth Amendment – Self-Incrimination

*Swinson v. State*, S21A0396, 2021 WL 769457 (Ga. Sup. Ct. Mar. 1, 2021)

The defendant was convicted of two murders. On appeal, he challenged, among other things, the denial of his motion to suppress evidence obtained from a search warrant based, in part, on a warrantless request for cell site information under the

SCA. He also argued ineffective assistance of counsel. The Georgia Supreme Court affirmed. It rejected the defendant's reliance on the United States Supreme Court decision in *Carpenter v. United States* (*q.v.*). *Carpenter* was decided three years after the motion to suppress had been denied, there was no binding appellate precedent at that time that imposed a warrant requirement, law enforcement acted in good faith in relying on exigent circumstances when it applied for the SCA order, and suppression would not deter future violations of the privacy interests recognized in *Carpenter*. The court also rejected the ineffective assistance of counsel claim because the defendant's trial counsel had essentially made the arguments accepted in *Carpenter* that had been rejected previously and the defendant did not identify any other arguments that his counsel should have made.

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Exigent Circumstances

#SCA

#Sixth Amendment – Assistance of Counsel

## DECISIONS – FOREIGN

Press Release No 29/21, *H.K. v. Prokuratuur*, Case C-746/18 (Court of Justice of the European Union (Mar. 2, 2021), Access, for purposes in the criminal field, to a set of traffic or location data in respect of electronic communications, allowing precise conclusions to be drawn concerning a person's private life, is permitted only in order to combat serious crime or prevent serious threats to public security (europa.eu)

#International

Press Release No 123/20, Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, et al.*, Court of Justice of the European Union (Oct. 6, 2020), The Court of Justice confirms that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security (europa.eu)

#International

## STATUTES, REGULATIONS, ETC. – FEDERAL

"(U) Clarification of information briefed during DIA's 1 December briefing on CTD," Central Intelligence Agency (unclassified: Jan. 15, 2021), https://int.nyt.com/data/documenttools/dni-to-wyden-on-commercially-available-smartphone-locational-data/5d9f9186c07993b6/full.pdf

#CSLI

#Fourth Amendment – Warrant Required or Not

#SCI

White Paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, Dep't's of Commerce and Justice and Office of the Dir. of Nat'l Intelligence (Sept. 2020), Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (commerce.gov)

#International

#Miscellaneous

"Privacy Risk Assessment for the U.S. Border Patrol Digital Forensics Program," DHS (July 30, 2020), DHS/CBP/PIA-053(a) U.S. Border Patrol Digital Forensics Programs

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

Inspector General for Tax Administration, Letter to Senators Wyden and Warren on use of location information from commercial databases, Dep't of Treasury (Feb. 18, 2021), Response.pdf (wsj.net)

#CSLI

#Fourth Amendment – Warrant Required or Not

#SCA

Private Industry Notification, "Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations," FBI (Mar. 10, 2021), FBI PIN: Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations | WaterISAC

#International

#Miscellaneous

FCC Enforcement Advisory, "Warning: Amateur and Personal Radio Licensees and Operators May Not Use Radio Equipment to Commit or Facilitate Criminal Acts," FCC Public Notice (released Jan. 17, 2021), Amateur & Personal Radio Users Reminded Not to Use Radios in Crimes | Federal Communications Commission (fcc.gov)

#Miscellaneous

"Privacy and Civil Liberties Oversight Board, "Report on Executive Order 12333" (Apr. 2, 2021), Oversight Reports - PCLOB

#Encryption

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

## STATUTES, REGULATIONS, ETC. – STATE

Press Release, "Governor Baker Signs Police Reform Legislation" (Mass. Governor's Press Office (Dec. 31, 2020), https://www.mass.gov/news/governor-baker-signs-police-reform-legislation

#Fourth Amendment – Warrant Required or Not

Michigan Constitution, Section 11 Searches and Seizures:

> The person, houses, papers, possessions, electronic data, and electronic communications of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things or to access electronic data or electronic communications shall issue without describing them, nor without probable cause, supported by oath or affirmation. The provisions of this section shall not be construed to bar from evidence in any criminal proceeding any narcotic drug, firearm, bomb, explosive or any other dangerous weapon, seized by a peace officer outside the curtilage of any dwelling house in this state. [Approved Nov. 3, 2020, Eff. Dec. 19, 2020].

http://legislature.mi.gov/doc.aspx?mcl-Article-I-11

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Directive #07-21, "Guidance on the Use of Visual Aids during Closing Arguments (Criminal)," N.J. Admin. Office of the Courts (Feb. 23, 2021), Directive #07-21 – Guidance on the Use of Visual Aids During Closing Arguments (Criminal) (njcourts.gov)

#Admissibility

#Trial-Related

## STATUTES, REGULATIONS, ETC. – FOREIGN

None.

## ARTICLES

S. Airey, *et al.*, "Approaching Self-Reporting & Co-operation Standards in U.S., U.K. and French Enforcement," Paul Hastings (Dec. 15, 2020), Paul Hastings LLP - Approaching Self-Reporting & Co-operation Standards in U.S., U.K. & French Enforcement

#Miscellaneous

L. Becker & A. Walsh, "New Criminal Rule 5(f) Firms Up Prosecutor Brady Obligations," Law360 (Jan. 27, 2021), https://www.law360.com/articles/1347642/new-criminal-rule-5-f-firms-up-prosecutor-brady-obligations

#Discovery Materials

#Miscellaneous

#Trial-Related

K. Broda-Bahm, "Don't Assume a Civil Zoom Trial Creates Reversible Error," Persuasive Litigator (Sept. 28, 2020), Don't Assume a Civil Zoom Trial Creates Reversible Error | Persuasive Litigator

#Trial-Related

L.J. Cameron, et al., "Courts Adopt Varying Approaches to Implementing Due Process Protections Act," *Subject to Inquiry* (McGuire Woods: Apr. 1, 2020), Courts Adopt Varying Approaches to Implementing Due Process Protections Act | Subject to Inquiry

#Discovery Materials

#Miscellaneous

#Trial-Related

Client Alert, "SFO Investigation Powers Over Foreign Companies Limited by U.K. Supreme Court Decision," Crowell & Moring (Mar. 3, 2021), SFO Investigation

Powers Over Foreign Companies Limited by U.K. Supreme Court Decision | Data Law Insights (crowelldatalaw.com)

#International

P. Egan, "Michigan Lawmakers Call for Change in Encrypted Police App," Detroit Free Press (Feb. 2, 2021), Michigan Lawmakers Call for Change in Encrypted Police App (govtech.com)

#Discovery Materials

#Encryption

#Miscellaneous

J.C. Giancario, *et al.*, "DOJ Issues Cryptocurrency Enforcement Framework, *Willkie Compliance* (Oct. 28, 2020), DOJ Issues Cryptocurrency Enforcement Framework | Insight (willkie.com)

#Miscellaneous

G.M. Graff, "The Furious Hunt for the MAGA Bomber," WIRED (Aug. 12, 2020), The Furious Hunt for the MAGA Bomber | WIRED

#CSLI

P. Grosdidier, "Tracking Traffic: You Think No One Knows Where You Are Driving? Think Again," Tex. Bar. J. 656 (Oct. 2020), State Bar of Texas | Articles (texasbar.com)

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

D. Harwell & C. Timberg, "How America's Surveillance Networks Helped the FBI Catch the Capitol Mob," *Washington Post* (Apr. 2, 2021), The FBI's Capitol riot investigation used surveillance technology that advocates say threatens civil liberties - The Washington Post

#CSLI

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#SCA

B.M. Heberlig, B.C. Bishop & N.P. Silverman, "The Due Process Protections Act: A New Opportunity for Defense Counsel to Advocate for Broad and Meaningful Brady Orders in Criminal Cases," Steptoe (Jan. 27, 2021), The Due Process Protections Act: A New Opportunity for Defense Counsel to Advocate for Broad and Meaningful Brady Orders in Criminal Cases | Steptoe & Johnson LLP

#Discovery Materials

#Miscellaneous

#Trial-Related

R.J. Hedges, G. Gottehrer & J.C. Francis IV, "Artificial Intelligence and Legal Issues," Litigation (ABA: Oct 8. 2020), Artificial Intelligence and Legal Issues (americanbar.org)

#Discovery Materials

#Miscellaneous

K. Hill, "How One State Managed to Actually Write Rules on Facial Recognition," N.Y. Times (posted: Feb. 27, 2021), How One State Managed to Actually Write Rules on Facial Recognition - The New York Times (nytimes.com)

#Fourth Amendment – Warrant Required or Not

C. Histed, D. Moore & D.C. Wolf, "Bot or Not? Authenticating Social Media Evidence at Trial in the Age of Internet Fakery," K&L Gates (Nov. 10, 2020), Bot or Not? Authenticating Social Media Evidence at Trial in the Age of Internet Fakery | HUB | K&L Gates

#Admissibility

A. Iftimie, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," Lawfare (Apr. 19, 2021), No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims - Lawfare (lawfareblog.com)

#Miscellaneous

L.E. Jehl, *et al.*, "Uber Criminal Complaint Raises the Stakes for Breach Response," McDermott Will & Emery (Aug. 31, 2020), Uber Criminal Complaint Raises the Stakes for Breach Response (mwe.com)

#Miscellaneous

J. Lynch & N. Sobel, "New Federal Court Rulings Find Geofence Warrants Unconstitutional," Electronic Frontier Foundation (Aug. 31, 2020), New Federal Court Rulings Find Geofence Warrants Unconstitutional | Electronic Frontier Foundation (eff.org)

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Particularity Requirement and/or Overbreadth

R. Mac, *et al.*, "Surveillance Nation," *BuzzFeed News* (Apr. 6, 2021), Clearview AI Offered Thousands Of Cops Free Trials (buzzfeednews.com)

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

C. Metz, "Police Drones are Starting to Think for Themselves," New York Times (Dec. 5, 2020), Police Drones Are Starting to Think for Themselves - The New York Times (nytimes.com)

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

C. Miller, "How Complete is "Complete" When It Comes to Digital Evidence?" Forensic Horizons (Sept. 15, 2020), How Complete is "Complete" When It Comes to Digital Evidence? | by Christa Miller | Forensic Horizons | Medium

#Admissibility

#Trial-Related

E. Nakashima & R. Albergotti, "The FBI Wanted to Unlock the San Bernadino Shooter's iPhone, It Turned to a Little-Known Australian Firm," *Washington Post*

(Apr. 14, 2021), Australian firm Azimuth unlocked the San Bernardino shooter's iPhone for the FBI - The Washington Post

#Encryption

L.H. Newman, "How Law Enforcement Gets Around Your Smartphone's Encryption," WIRED (Jan. 15, 2021), How Law Enforcement Gets Around Your Smartphone's Encryption | WIRED

#Encryption

A. Ng, "Google is Giving Data to Police Based on Search Keywords, Court Docs Show," CNET (Oct. 8, 2020), Google is giving data to police based on search keywords, court docs show - CNET

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Third-Party Doctrine

T.A. Pickles, "CPRA Creates New Obligations and Questions for Businesses in Connection with Criminal Investigations," GT Alert Greenberg Traurig (Nov. 12, 2020), CPRA Creates New Obligations and Questions for Businesses in Connection with Criminal Investigations | Insights | Greenberg Traurig LLP (gtlaw.com)

#Miscellaneous

#Reasonable Expectation of Privacy

A.C. Raul & R.D. Klinger, "U.S. Government White Paper to Help Companies Address the EU's National Security Concerns in Schrems II," Sidley (Sept. 30, 2020), Data Matters Privacy Blog U.S. Government White Paper to Help Companies Address the EU's National Security Concerns in Schrems II - Data Matters Privacy Blog (sidley.com)

#International

#Miscellaneous

T. Riley, "Extremists Flocking to Encrypted Apps Could Restart Debate Over Law Enforcement Access," The Cybersecurity 202, Washington Post (Jan. 13, 2021),

The Cybersecurity 202: Extremists flocking to encrypted apps could restart debate over law enforcement access - The Washington Post

#Encryption

J. Rubino, "WhatsApp, Signal, Telegram and iMessage: Choosing a Private Encrypted Chat App," DollarCollapse.com (Jan. 14, 2021), WhatsApp, Signal, Telegram and iMessage: Choosing a Private Encrypted Chat App - DollarCollapse.com

#Encryption

J. Schuppe, "She Didn't Know Her Kidnapper. But He was Using Google Maps – and That Cracked the Case," NBC News (Dec. 29, 2020), https://www.nbcnews.com/news/us-news/she-didn-t-know-her-kidnapper-he-was-using-google-n1252472

#CSLI

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

C. Warzel & S.A. Thompson, "They Stormed the Capitol. Their Apps Tracked Them," N.Y. Times (posted Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html

#CSLI

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

D.M. West, "Digital Footprints are Identifying Capitol Rioters," Brookings Tech Tank (Jan. 19, 2021), Digital fingerprints are identifying Capitol rioters (brookings.edu)

#CSLI

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

Z. Whittaker, "Minneapolis Police Tapped Google to Identify George Floyd Protesters," Yahoo.com (Feb. 6, 2021), Minneapolis police tapped Google to identify George Floyd protesters (yahoo.com)

#CSLI

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

## OTHER PUBLICATIONS

M. Caldwell, *et al*., "AI-Enabled Future Crime," Crime Sci. 9 (2020), AI-enabled future crime | Crime Science | Full Text (biomedcentral.com)

#Miscellaneous

T. Christakis & F. Terpan, "EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options," Evidence & Evidentiary Procedure eJournal (posted Feb. 3, 2021), EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options by Theodore Christakis, Fabien Terpan :: SSRN

#International

Press Release, *Justice Dept. Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities*, (USDOJ Office of Pub. Affairs: Apr. 13, 2021), Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities | OPA | Department of Justice

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

O. S. Kerr, "The Fourth Amendment Limits of Internet Content Preservation," St. Louis U. L. J., Forthcoming (posted Dec. 18, 2020), The Fourth Amendment Limits of Internet Content Preservation by Orin S. Kerr :: SSRN

#Fourth Amendment – Warrant Required or Not

#Preservation and Spoliation

L. Koepke, *et al.*, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," Upturn (Oct. 2020),

https://www.upturn.org/reports/2020/mass-extraction/#:~:text=without%20meaningful%20consent.-,To%20search%20phones%2C%20law%20enforcement%20agencies%20use%20mobile%20device%20forensic,can%20then%20be%20programmatically%20searched

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

C.D. Linebaugh & E.C. Liu, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Cong. Research Serv. (Mar. 17, 2021), https://crsreports.congress.gov/product/pdf/R/R46724

#International

"Privacy Protections in State Constitutions" Nat'l Conference of State Legislatures (Nov. 6, 2020), Privacy Protections in State Constitutions (ncsl.org)

#Fourth Amendment – Warrant Required or Not

#Miscellaneous